

# Analisis Tingkat Kematangan Keamanan Sistem Informasi Universitas Negeri Manado menggunakan Framework COBIT 2019

Billy Tampilang<sup>1</sup>, Keith Francis Ratumbuisang<sup>2</sup>, Johan Reimon Batmetan<sup>3</sup>

<sup>1,2,3</sup> Jurusan Pendidikan Teknologi Informasi dan Komunikasi, Fakultas Teknik, Universitas Negeri Manado

Correspondent Author :

[tampilangbilly@gmail.com](mailto:tampilangbilly@gmail.com)

**Abstract** — The academic information system contains crucial data such as academic information, employee data, research, and administrative documents. Cybercrimes in the 4.0 era, including data theft and system hacking, are increasingly prevalent with advancing technology. This study aims to comprehensively measure the maturity level of the information system network security at Universitas Negeri Manado using the COBIT 2019 Framework in the DSS05 domain (Ensure Systems Security). The method used is descriptive quantitative analysis, involving data collection through questionnaires and interviews, and data processing using the CMMI (Capability Maturity Model Integration) method. The findings of this study indicate that the maturity and security levels of network services vary based on the seven processes in the DSS05 domain. The DSS05.01 process (Protecting Against Malicious Software) has a maturity level of 3.90, DSS05.02 (Managing Vulnerabilities) reaches 4.90, DSS05.03 (Managing Physical System Security) reaches 4.70, DSS05.04 (Managing Identity and Access) reaches 4.60, DSS05.05 (Protecting Against External Attacks) reaches 3.60, DSS05.06 (Managing Security Incidents) reaches 3.70, and DSS07 (Managing Vulnerabilities and Monitoring Infrastructure for Security-Related Events) reaches a maturity level of 3.10. Overall, the analysis findings in this study reach 4.35, indicating that the network security maturity level at Universitas Negeri Manado is quite good but still requires some improvements to reach the desired level.

**Keyword** — Information System, COBIT 2019, Maturity Level, CMMI.

**Abstrak** — Sistem Informasi akademik memuat data – data penting seperti informasi akademik, data kepegawaian, penelitian dan dokumen administrasi. Kejahatan cyber pada era 4.0 berupa pencurian data dan perhackingan terhadap sistem semakin marak dengan teknologi yang semakin canggih. Tujuan penelitian ini adalah untuk mengukur secara komprehensif tingkat kematangan keamanan jaringan Sistem Informasi di Universitas Negeri Manado dengan menggunakan Framework COBIT 2019 pada Domain DSS05 (Ensure Systems Security). Metode yang digunakan adalah Analisis kuantitatif deskriptif yang melibatkan pengumpulan data lewat kusioner dan wawancara, serta pengolahan data menggunakan metode CMMI (Capability Maturity Model Integration). Hasil temuan pada penelitian ini menunjukkan bahwa tingkat kematangan dan keamanan layanan jaringan bervariasi berdasarkan 7 proses pada domain DSS05. Proses DSS05.01 (Melindungi dari perangkat lunak berbahaya) memiliki tingkat kematangan 3.90, DSS05.02 (Mengelola Kerentanan) mencapai 4.90, DSS05.03 (Mengelola Keamanan Sistem Fisik) mencapai 4.70, DSS05.04 (Mengelola akses identitas dan hak) mencapai 4.60, DSS05.05 (Melindungi dari serangan eksternal) pada 3.60, DSS05.06 (Mengelola insiden keamanan) mencapai 3.70 dan DSS07 (Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan) mencapai tingkat kematangan 3.10. Secara keseluruhan

hasil temuan analisis pada penelitian ini mencapai 4.35 yang menunjukkan bahwa tingkat kematangan keamanan jaringan di Universitas Negeri Manado sudah berada pada tahap yang cukup baik namun masih memerlukan beberapa peningkatan untuk mencapai level yang diharapkan.

**Kata kunci** — Sistem Informasi, COBIT 2019, Tingkat Kematangan, CMMI.

## I. PENDAHULUAN

Dari waktu ke waktu, kemajuan teknologi dan informasi membawa perubahan yang cukup besar. Dengan melihat sistem kehidupan manusia sehari-hari, seperti berkomunikasi, berinteraksi, bekerja, dan melihat kegiatan manusia lainnya, baik yang melibatkan individu maupun banyak orang (kelompok), kita dapat mengetahui perubahan tersebut. Saat ini, semua orang membutuhkan pengolah data dan media informasi untuk melakukan segala aktivitas sehari-hari dalam segala aspek kehidupan. Saat ini, semua serba terbuka dan serba cepat, dan dengan adanya berbagai macam media informasi, semua orang memiliki banyak pilihan untuk mencari atau mengetahui sesuatu yang ingin mereka ketahui dengan cepat tanpa memerlukan waktu yang lama. Informasi sangat penting untuk kehidupan manusia, terutama untuk institusi, karena semua kegiatan yang dilakukan memerlukan informasi yang cepat untuk menyelesaikan tugas-tugasnya. Dalam dunia pendidikan, sistem informasi dimanfaatkan untuk manajemen dan mengelolah data. Saat ini sistem informasi juga tidak hanya digunakan sebagai alat bantu pembelajaran atau hanya sebagai media pembelajaran, melainkan juga digunakan untuk membantu proses penilaian akademik, penyebaran informasi dan lain sebagainya. Berdasarkan hal ini, tidak bisa dipungkiri bahwa teknologi sudah menjadi modal utama dalam pembelajaran yang ada mulai dari jenjang sekolah dasar hingga perguruan tinggi. Khususnya di Jurusan Pendidikan Teknologi Informasi dan Komunikasi, Universitas Negeri Manado, sistem informasi sangat diperlukan untuk mempermudah akses informasi dari, manajemen dokumen dan mempermudah admistrasi yang ada di dalam. Salah satu permasalahan yang masih banyak terjadi di Pendidikan Teknologi Informasi dan Komunikasi yaitu proses bimbingan skripsi yang tidak terdokumentasi. Skripsi adalah mata kuliah yang harus diselesaikan oleh mahasiswa sebelum mereka tamat dari perguruan tinggi. Skripsi merupakan salah satu syarat terakhir yang harus diselesaikan oleh siswa strata 1 (S1) sebelum mendapatkan gelar sarjana. Mahasiswa diharuskan untuk memilih dan

---

mengusahakan topik tertentu yang memiliki tingkat kesulitan yang sesuai dengan apa yang telah mereka pelajari. Skripsi ini pasti akan dilakukan oleh mahasiswa sendiri. Fakultas atau program studi secara bijak akan mempercayakan mahasiswa pada seorang dosen untuk membimbing mereka dalam menyelesaikan tugas akhir mereka. Ini akan memastikan bahwa mahasiswa layak untuk wisuda. Tentunya ada banyak proses yang terlibat dalam menyelesaikan tugas akhir, mulai dari administrasi, bimbingan, pembuatan proposal hingga penilaian.

Proses bimbingan skripsi diperlukan untuk mengoreksi kesalahan-kesalahan dalam proses penyusunan skripsi. Selama ini proses bimbingan tidak terdokumentasi dengan baik, sehingga dosen dan mahasiswa kurang terarah ketika bimbingan. Adapun kartu bimbingan skripsi masih manual dan diisi hanya untuk persyaratan ujian. Salah satu solusi yaitu dengan mengimplementasikan sistem informasi bimbingan skripsi bisa mempermudah administrasi yang ada di Pendidikan Teknologi Informasi dan Komunikasi.

Berdasarkan uraian yang ada diatas maka penulis mengambil judul “Pengembangan Sistem Informasi Bimbingan Skripsi Jurusan Pendidikan Teknologi Informasi Dan Komunikasi”. Sistem Informasi perguruan tinggi pada umumnya memuat informasi terkait data akademik, data peneliti dan data dosen (Indaryani, 2013.). Oleh karena itu sangat diperlukan suatu sistem keamanan yang proaktif dan komprehensif serta sulit dibobol oleh kejahatan cyber. Kejahatan cyber pada sistem informasi umumnya dilakukan untuk upaya memperoleh dan menyalahgunakan data atau mengambil alih kendali pengelolaan data untuk tujuan kejahatan (Arisandy Oktafian Yogi, 2020). Penelitian oleh (Rahmawati Ineu, 2017) mengemukakan bahwa ancaman kejahatan siber (cyber crime) dalam bentuk pencurian informasi dan data yang bersifat rahasia ditujukan untuk menyerang individu, instansi pemerintah, militer dan bahkan perguruan tinggi telah mengancam pertahanan suatu negara khususnya pada bagian keamanan sistem. Demikian juga studi yang dilakukan oleh (Abidin Zainil Dodo, 2015) bahwa cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Hasil – hasil studi ini menyiratkan akan adanya potensi penyerangan sistem informasi didunia Pendidikan terutama perguruan tinggi.

Dalam dunia teknologi yang terus berubah, keamanan sistem informasi sangat penting, terutama di institusi pendidikan seperti universitas untuk menjaga integritas dan ketahanannya karena sistem ini berfungsi sebagai pusat operasional administratif, kegiatan akademis, dan pengelolaan data (Siddiq Susilo, 2013). Universitas melakukan banyak hal, termasuk mendukung pendidikan, penelitian, dan inovasi. Sistem informasi di institusi sangat penting untuk memudahkan berbagai tugas, seperti pendaftaran siswa dan pengelolaan keuangan, serta penyimpanan platform kolaborasi dan data penelitian (Sudipa

Iwan, 2023). Namun, peningkatan kompleksitas sistem dikombinasikan dengan meningkatnya bahaya cyber sehingga menimbulkan masalah yang signifikan (Othman Amarmuazam, 2017). Kemajuan teknologi yang terus berubah menjadi tantangan utama, bagi keamanan cyber yang terus berkembang juga kerentanan terhadap sistem keamanan menjadi hal yang krusial terutama pada institusi perguruan tinggi sehingga perlu peningkatan dalam manajemen keamanan sistem informasi termasuk sistem informasi di perguruan tinggi. Dalam konteks ini, penelitian ini berfokus pada studi keamanan sistem informasi di Universitas Negeri Manado (UNIMA) yang mengaplikasikan COBIT 2019 pada Domain DSS05. Pada dasarnya COBIT 2019 menawarkan pedoman terbaik dan praktik untuk menyelaraskan TI pada sistem di Institusi perguruan tinggi. (Nachrowi Erika, 2020).

Dari pengamatan awal peneliti, sesuai pengalaman peneliti sebagai salah satu pengguna layanan sistem informasi ini, dan wawancara awal dengan pengelolanya diperoleh informasi bahwa Sistem Informasi di Universitas Negeri Manado sering menghadapi beberapa masalah, terutama kesalahan perangkat lunak dan perangkat keras dan protokol keamanan yang tidak memadai adalah semua potensi ancaman yang signifikan. Sistem Informasi di Universitas Negeri Manado pada selang waktu tahun ajaran 2022 / 2023 pernah mengalami pembobolan pada bagian jaringan dan hosting dari orang yang tidak bertanggungjawab sehingga mengakibatkan beberapa kendala dalam pemakaian layanan sistem informasi. Untuk mengatasi masalah ini, perlu dilakukan pemeriksaan menyeluruh terhadap keamanan sistem, menemukan kerentanan, dan membuat saran yang dapat ditindaklanjuti.

Melihat hal tersebut maka penting untuk menambah tingkat keamanan dalam universitas melalui kebutuhan akan suatu kerangka kerja atau framework yang terstruktur untuk mengelola dan meningkatkan keamanan sistem informasi. Dalam konteks ini COBIT 2019 merupakan pilihan yang tepat karena memberikan panduan secara terstruktur dalam mengelola resiko dan keamanan sistem informasi. Penelitian ini berfokus pada domain DSS05 (Delivery, Service, and Support) yang merupakan bagian dari COBIT 2019. Domain DSS05 mencakup manajemen layanan keamanan, pengelolaan insiden keamanan dan pengelolaan sistem keamanan. Oleh karena itu penelitian ini akan memberikan kontribusi dalam menganalisis, mengevaluasi dan memberikan rekomendasi sistem informasi di Universitas Negeri Manado, khususnya pada aspek-aspek yang tercakup dalam domain DSS05.

Berdasarkan uraian informasi diatas maka akan diangkat Penelitian yang berjudul : Analisis Tingkat Kematangan Keamanan Sistem Informasi Universitas Negeri Manado Menggunakan Framework COBIT 2019. Penelitian ini diharapkan dapat memiliki dampak yang signifikan pada pengelolaan sistem informasi berdasarkan Cobit 2019 dengan Domain DSS05..

---

## II. KAJIAN TEORI

### A. Sistem Informasi

Sistem adalah suatu kesatuan yang terdiri atas komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi, atau energi (Hapzi, 2019). Dalam konteks sistem informasi, sistem merupakan gabungan yang terorganisasi dari manusia, perangkat lunak, perangkat keras, jaringan komunikasi, dan sumber data dalam mengumpulkan, memproses, menyimpan, dan menyajikan informasi. Informasi adalah data yang disimpan, diproses, atau ditransmisikan. Informasi memiliki beberapa ciri-ciri, seperti benar atau salah. Informasi berhubungan dengan kebenaran atau kesalahan terhadap kenyataan. Informasi harus benar-benar baru bagi si penerima. Tambahan: Informasi dapat memperbarui atau memberikan perubahan terhadap informasi yang telah ada. Korektif: Informasi dapat digunakan untuk melakukan koreksi terhadap informasi sebelumnya yang salah. Informasi memiliki sumber yang dapat diverifikasi. Sistem informasi adalah sebuah sistem formal, sosioteknikal, dan organisasional yang dirancang untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi. Dari perspektif sosioteknis, sistem informasi disusun oleh empat komponen: tugas, orang, struktur (atau peran), dan teknologi. Sistem informasi memiliki tujuan untuk memproses, mengumpulkan, menyimpan, dan menyajikan informasi guna mendukung pengambilan keputusan dan mengelola operasi suatu organisasi.

### B. COBIT 2019

COBIT 2019 adalah suatu kerangka kerja (framework) yang dirancang oleh Information Systems Audit and Control Association (ISACA) untuk membantu organisasi dalam mengelola, mengendalikan, dan mengukur efektivitas penggunaan teknologi informasi (TI). COBIT sendiri merupakan singkatan dari Control Objectives for Information and Related Technologies. Implementasi COBIT (Control Objectives for Information and Related Technologies) di perguruan tinggi bertujuan untuk meningkatkan pengelolaan dan pengendalian teknologi informasi dengan fokus pada pencapaian tujuan bisnis dan keamanan informasi (Aziz, Kusriani, dan Nasiri 2023). COBIT dirancang untuk membantu institusi pendidikan tinggi dalam mengelola risiko, memastikan kepatuhan terhadap regulasi, serta meningkatkan kinerja dan efisiensi sistem informasi (Aziz, Kusriani, dan Nasiri 2023).

### C. Deliver, Service, and Support (DSS05)

DSS05 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 (ISACA, 2012). Base Practices dan Work Product berdasarkan penilaian proses ini adalah Dokumen Prosedur Operasi Instalasi dan Monitoring Software, kegiatan klasifikasi data, Log Firewall dan Antivirus, Dokumen Prosedur Operasi Hak Akses, Dokumen prosedur Operasi Lisensi Software serta

Dokumen Prosedur Operasi Pengamanan TI. Selain itu, terdapat juga pelaksanaan klasifikasi data yang telah dilaksanakan namun belum ditemukan dokumen tertulis yang menjelaskan klasifikasi data yang dilakukan oleh perusahaan. Delivery, Service and Support (DSS), meliputi mengirimkan, service atau layanan, dan dukungan atau memberi pelayanan yang aktual bagi bisnis, termasuk manajemen data dan proteksi informasi yang berhubungan dengan proses bisnis.

DSS merupakan domain COBIT 2019 yang berhubungan dengan operasional IT, seperti pemberian layanan, pengelolaan keamanan dan kontinuitas, dukungan layanan pengguna, dan pengelolaan data dan fasilitas operasional. Dalam domain DSS terdapat 7 Sub-domain sebagai berikut :

1. Protect against malware (DSS05.01)  
Melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada diseluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak.
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 endpoint security (DSS05.03)  
Memberikan kepastian terhadap titik akhir keluaran (end poin) (misal: Laptop, desktop, dan server) dijamin tingkat yang sama atau lebih besar dari persyaratan keamanan yang disetujui.
4. Manage user identity and logical access (DSS05.04)  
Memberikan kepastian terhadap semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis. Mereka dan berkoordinasi dengan divisi bisnis yang mengelola hak akses.
5. Manage physical access to IT assets (DSS05.05)  
Menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan fisik. Bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau.
6. Manage sensitive documents and output devices (DSS05.06)  
Menetapkan pengamanan fisik. Dalam segi dokumen yang berhubungan dengan instansi. Sehingga semua keluaran dokumen terstandar dalam keamanan.
7. Monitor the infrastructure for security-related events (DSS05.07)  
Menggunakan alat deteksi intrusi, untuk memantau infrastruktur untuk hak akses yang tidak sah dan memastikan setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian

### D. CMMI (Capability Maturity Model Integration)

Maturity model adalah suatu metode untuk mengukur level pengembangan manajemen proses, yang berarti adalah mengukur sejauh mana kapabilitas manajemen

tersebut. (Sufyana Mecca Candra dan Suharto Edi, 2018). Tujuan penggunaan CMMI dalam suatu institusi adalah untuk meningkatkan proses pengembangan dan penyempurnaan produk perangkat lunak institusi tersebut. CMMI mempunyai Tingkat Kemampuan. Tingkat Kapabilitas merupakan model untuk menggambarkan bagaimana setiap proses inti berjalan dalam suatu institusi.

Capability Maturity Model Integration (CMMI) adalah model yang membantu organisasi untuk meningkatkan kematangan proses mereka. Terdapat lima tahapan dalam CMMI, yaitu Initial, Managed, Defined, Quantitatively Managed, dan Optimizing. Berikut adalah penjelasan singkat untuk setiap tahapan tersebut:

1. Initial (Tahap Awal)

Pada tahap ini, organisasi biasanya memiliki pendekatan yang tidak terorganisir atau bahkan acak terhadap manajemen proyek dan proses. Tidak ada standar yang diterapkan dan kinerja proyek bergantung pada keahlian individu. Ini adalah tingkat kematangan terendah.

2. Managed (Tahap Dikelola)

Organisasi di tingkat ini telah mulai menerapkan praktik manajemen dasar. Proses dasar telah didefinisikan dan dilaksanakan secara konsisten. Fokus utama pada manajemen proyek dan penerapan standar.

3. Defined (Tahap Terdefinisi):

Pada tahap ini, organisasi memiliki proses terdefinisi dengan baik. Proses tersebut terdokumentasi secara lengkap, dan ada standar yang jelas untuk mengelola dan mengukur kinerja. Fokus pada pengembangan dan pemeliharaan sistem.

4. Quantitatively Managed (Tahap Dikelola secara Kuantitatif)

Organisasi di tingkat ini tidak hanya memiliki proses yang terdefinisi, tetapi juga dapat mengukur kuantitas dan kualitas kinerja mereka secara terus-menerus. Menerapkan metrik dan analisis data untuk meningkatkan kinerja.

5. Optimizing (Tahap Optimasi):

Pada tahap ini, organisasi terus meningkatkan proses mereka melalui pemantauan dan analisis yang mendalam. Mereka fokus pada inovasi, efisiensi, dan peningkatan berkelanjutan. Mencari cara untuk mengoptimalkan proses secara terus-menerus.

Setiap tahapan mencerminkan tingkat kematangan proses dalam organisasi, dengan tahap Optimizing sebagai tingkat tertinggi di mana organisasi mencapai puncak kematangan dalam penerapan dan pengelolaan proses. Proses peningkatan kematangan di CMMI membantu organisasi untuk menjadi lebih efisien, efektif, dan responsif terhadap perubahan.

### III. METODE PENELITIAN

#### A. Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif untuk menganalisis tingkat kematangan keamanan sistem informasi berdasarkan framework COBIT 2019 di lingkungan Universitas Negeri Manado. Pendekatan kuantitatif digunakan untuk mengumpulkan data numerik yang akan dianalisis secara deskriptif. Metode deskriptif kuantitatif digunakan karena metode ini dilakukan dengan tujuan utama untuk membuat gambaran atau mendeskripsikan suatu keadaan secara objektif (Prasko, Santoso, & Sutomo, 2016, hlm.54).

#### B. Teknik Pengumpulan Data

1. Wawancara

Data dalam penelitian ini diperoleh sebagai data primer dari hasil wawancara dengan informan pengelolaan Sistem Informasi Universitas Negeri Manado dengan tujuan untuk mendapatkan informasi awal mengenai kondisi dan situasi yang terjadi di UPA TIK Universitas Negeri Manado. Adapun kriteria informan adalah memiliki kompetensi IT, berpengalaman mengelola IT selama 3 tahun terakhir dan ditunjuk oleh ketua UPA TIK.

2. Adaptasi Kuisisioner

Adaptasi Kuisisioner merupakan penggunaan kuisisioner terstruktur yang diadaptasi untuk mengumpulkan data kuantitatif dengan tujuan untuk mendapatkan respons dari responden terkait dimensi kematangan keamanan sistem informasi (Eneng Nurlaili Wangi dkk, 2023). Kuisisioner akan dibagikan kepada pihak IT Universitas Negeri Manado yang memiliki kompetensi IT, berpengalaman mengelola IT selama 3 tahun terakhir.

3. Studi Literatur

Studi Literatur yang dilakukan adalah pencarian dan analisis terkait dengan COBIT 2019, domain DSS05, CMMI, dan topik keamanan sistem informasi dengan tujuan mendapatkan landasan teoritis, kerangka konseptual, dan pemahaman mendalam tentang konsep keamanan sistem informasi dan implementasinya dalam konteks Universitas. Analisis literatur akan mencakup studi dokumen, artikel ilmiah, dan sumber daya terpercaya lainnya untuk memberikan pandangan yang holistik.

#### C. Analisis Data

Kuisisioner

Sumber data kuisisioner diperoleh melalui adaptasi untuk mengumpulkan data kuantitatif dengan tujuan untuk mendapatkan respons dari responden terkait dimensi kematangan keamanan sistem informasi yang ada pada proses COBIT 2019 yaitu DSS05. Kuisisioner dibagikan kepada pihak pengelola IT yang mengelola Sistem Informasi Universitas Negeri Manado yang sudah ditentukan berdasarkan kriteria yang ditetapkan. Bentuk kuisisioner berupa 35 pernyataan yang ada pada Proses 7 DSS05 dengan pengukuran berdasarkan skala likert dimulai dari Tingkat 0 sampai 5. Hasil jawaban kuisisioner

akan diakumulasikan untuk mendapatkan capability level. Berikut adalah contoh tabel kuisioner:

Tabel 1. Penilaian Kusioner

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

Keterangan:

Pada kuisioner ini, penilaian dilakukan untuk tingkat kemampuan 0, 1, 2, 3, 4, dan 5 sesuai dengan pengukuran tingkat kematangan berdasarkan Capability Maturity Model Integration:

- Level 0: Non-existent
- Level 1: Initial/Ad hoc
- Level 2: Repeatable but intuitive
- Level 3: Defined process
- Level 4: Managed and measurable
- Level 5: Optimised

#### D. Pengolahan Data Model CMMI

Metode Perhitungan Maturity Level Menggunakan Model CMMI adalah pendekatan yang mengukur tingkat kematangan atau maturitas keamanan sistem suatu organisasi (Rusydi dkk). Model ini akan menghitung tingkat keamanan sistem informasi di Universitas Negeri Manado berdasarkan data yang diperoleh dari hasil wawancara dan hasil kuisioner. Rumus yang dipakai dalam perhitungan maturity level berdasarkan model CMMI adalah sebagai berikut:

$$\text{Indeks Kematangan} = \frac{\text{Jumlah Nilai Jawaban}}{\text{Total Nilai Kuesioner}}$$

Setelah didapatkan hasil perhitungan berdasarkan rumus di atas, hasil maturity tersebut akan dihitung dengan rumus berikut ini:

$$\text{Maturity Level DSS05} = \frac{\text{Maturity Level}}{\text{Banyak Proses}}$$

Hasil perhitungan maturity level berdasarkan rumus di atas akan menentukan nilai ketercapaian layanan keamanan jaringan sistem informasi Universitas Negeri Manado yang kemudian dapat merumuskan rekomendasi berdasarkan hasil perhitungan maturity level.

## IV. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengetahui Tingkat kematangan keamanan layanan jaringan sistem informasi Universitas Negeri Manado. Peneliti mengkaji tujuan ini dengan menerapkan metode analisis deskriptif kuantitatif dengan data berbasis kuisioner yang telah disebarkan dan wawancara dengan responden sebagai tindak lanjut atas pertanyaan kuisioner.

#### A. Validasi DSS05 Dengan Aspek Keamanan

Validasi ini merupakan Adaptasi dari penelitian sebelumnya yang dianalisis berdasarkan DSS05 pada framework COBIT 2019 dengan parameter keamanan yaitu Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability) seperti pada table 2.

Tabel 2. Validasi DSS05 dengan Aspek Keamanan

No	Kode DSS	C	I	A
1	DSS05.01	✓		
2	DSS05.02	✓		
3	DSS05.03	✓	✓	
4	DSS05.04	✓		✓
5	DSS05.05		✓	✓
6	DSS05.06		✓	✓
7	DSS05.07		✓	

#### B. Hasil Pengolahan Data

Analisis dan interpretasi data wawancara dan kuisioner 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 3. Nilai Kriteria Maturity Level

Level	Kriteria	Keterangan
0	0 – 0,50	Initial
1	0,51 – 1,50	Ad Hoc
2	1,51 – 2,50	Repeatable But Intuitive
3	2,51 – 3,50	Define Process
4	3,51 – 4,50	Managed and Measurable
5	4,51 – 5,00	Optimized

Hasil dari kuisioner yang telah di berikan terhadap responden dan telah di isi oleh responden di dapatkan hasil seperti pada Tabel 4.

Tabel 4. Perhitungan Maturity Level

Total Pernyataan	Jumlah Responden	Total Pernyataan x Jumlah Responden	Total Nilai Kuesioner	Jumlah Nilai Jawaban
Pihak Pengelola TI Unima				
5	4	20	20	78
5	4	20	20	98
5	4	20	20	95
5	4	20	20	92

4	4	16	16	73
6	4	24	24	90
5	4	20	20	82
Indeks Kematangan = Jumlah nilai jawaban: Total nilai kusioner				
3,9		3,9		
4,9		4,9		
4,75		4,75		
4,6		4,6		
4,56		4,5		
3,75		3,75		
4,1		4,1		

Dari Perhitungan indeks kematangan terhadap data kusioner didapatkan hasil seperti table berikut ini :

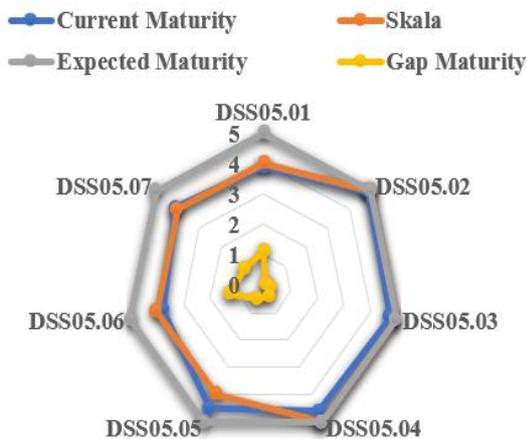
$$\text{Indeks Kematangan} = \frac{\text{Jumlah Nilai Jawaban}}{\text{Total Nilai Kuesioner}}$$

Tabel 5. Hasil Indeks / Maturity Level

DSS05	Jumlah Jawaban	Jumlah Pernyataan	Indeks / Maturity level saat ini
01	78	5	3,9
02	98	5	4,9
03	95	5	4,75
04	92	5	4,6
05	73	4	4,5
06	90	6	3,75
07	82	5	4,1

Dari hasil indeks di atas akan dibandingkan antara maturity level saat ini dengan maturity target yang diharapkan sehingga didapatkan maturity GAP seperti pada gambar 1.

### Analisis GAP



Gambar 1. Diagram GAP Maturity Level

GAP maturity level pada gambar 1 menunjukkan bahwa Expected Maturity atau nilai maturity yang diharapkan adalah level yang bernilai 5 sedangkan hasil output dari indeks berada pada level yang bernilai 4. Gap maturity level dapat dianalisis sehingga dapat ditetapkan maturity level pada setiap domain seperti pada table 6.

Tabel 6. GAP Maturity Level

Maturity Level				
Domain	Current Maturity	Skala	Expected Maturity	Gap Maturity
DSS05.01	3,9	4	5	1.10
DSS05.02	4,9	5	5	0.10
DSS05.03	4,75	5	5	0.30
DSS05.04	4,6	5	5	0.40
DSS05.05	4,5	4	5	0.50
DSS05.06	3,75	4	5	1.30
DSS05.07	4,1	4	5	0.90

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

$$\text{Maturity Level DSS05} = \frac{\text{Maturity Level}}{\text{Banyak Proses}}$$

$$\begin{aligned} & (DSS05.01) + (DSS05.02) + \\ & (DSS05.03) + (DSS05.04) + \\ & (DSS05.05) + (DSS05.06) + \\ & (DSS05.07) \end{aligned}$$

$$\text{Maturity Level DSS05} = \frac{\quad}{7}$$

$$3.9 + 4.9 + 4.75 +$$

$$\text{Maturity Level DSS05} = \frac{4.6 + 4.5 + 3.75 + 4.1}{7}$$

$$\text{Maturity Level DSS05} = 4.35$$

Dari hasil perhitungan maturity level diatas, hasil yang didapatkan bahwa nilai ketercapaian mencapai 4,35 yang menunjukkan Tingkat kematangan layanan keamanan jaringan sistem informasi Universitas Negeri Manado berada pada level 4 Managed and Measurable atau "Dikelola dan Dapat Diukur". Hal ini menunjukkan bahwa Universitas Negeri Manado telah memiliki proses keamanan yang terkelola dengan baik dan dapat diukur, tetapi masih memiliki ruang untuk terus meningkatkan keamanan jaringan sistem informasinya.

### C. Rekomendasi

Berdasarkan analisis Gap yang didapatkan dari hasil target level yang diharapkan dengan perbandingan level yang dicapai berdasarkan hasil perhitungan maturity level

pada COBIT 2019 Domain DSS05 saat ini ,maka rekomendasi yang dapat diberikan sebagai berikut :

1. DSS05.01: Melindungi dari Perangkat Lunak Berbahaya berada pada Level 4 (Managed). Rekomendasi yang diberikan adalah Gunakan AI dan machine learning, Implementasi continuous improvement cycle (PDCA) dan Pelatihan tim IT dalam teknologi baru
2. DSS05.02: Mengelola Keamanan Jaringan dan Konektivitas berada pada Level 5 (Optimized). Rekomendasi yaitu Pemantauan dan pemeliharaan rutin dan mengadopsi inovasi teknologi terbaru.
3. DSS05.03: Mengelola Keamanan Titik Akhir berada pada Level 5 (Optimized). Rekomendasi yang diberikan yaitu Pemantauan dan pemeliharaan rutin mengadopsi inovasi teknologi terbaru.
4. DSS05.04: Mengelola Identitas Pengguna dan Akses Logis berada pada Level 5 (Optimized). Rekomendasi yaitu Pemantauan dan pemeliharaan rutin dan mengadopsi inovasi teknologi terbaru.
5. DSS05.05: Mengelola Akses Fisik ke Aset IT berada pada Level 4 (Managed). Rekomendasi yang diberikan adalah Pelatihan staf, pembaruan infrastruktur, adopsi best practices.
6. DSS05.06: Mengelola Dokumen Sensitif dan Perangkat Keluaran berada pada Level 4 (Managed) Rekomendasi yang diberikan adalah Peningkatan aspek-aspek untuk efisiensi maksimal.
7. DSS05.07: Mengelola Kerentanan dan Memantau Infrastruktur untuk Kejadian Keamanan berada pada Level 4 (Managed) Peningkatan aspek-aspek untuk mencapai kategori "Optimized".

## V. KESIMPULAN

Hasil temuan penelitian diatas bukan merupakan yang pertama dalam penelitian dengan hasil yang hampir mencapai level 5 (Optimized), pada penelitian sebelumnya yang dilakukan oleh Rusydi Umar dkk dengan judul Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI) (HYPERLINK <http://ejournal.undip.ac.id/index.php/jsinbis>) juga menghasilkan hasil dengan level yang sama yaitu dengan nilai 4,45 (Managed and Measurable). Penelitian tersebut membahas tentang layanan keamanan jaringan pada Sistem Informasi di Universitas Ahmad Dahlan, Yogyakarta dengan menggunakan metode Analisis Deskriptif dan menggunakan metode CMMI untuk mengukur tingkat ketercapaian sehingga mendapatkan hasil dengan level yang sama yaitu dengan nilai 4,45 (Managed and Measurable). Hal ini memperkuat hasil temuan pada penelitian diatas bahwa pencapaian tingkat kematangan keamanan Sistem Informasi pada penelitian sebelumnya telah menunjukkan konsistensi dalam hasil yang tinggi, mengindikasikan bahwa Sistem Informasi yang diteliti telah memiliki proses yang terdefinisi dengan baik, dikelola, dan diukur secara efektif,

namun masih perlu sedikit peningkatan untuk mencapai level tertinggi (Optimized).

## DAFTAR ACUAN

- Arisandy Oktafian Yogi. 2020. Penegakan Hukum Terhadap Cyber Crime Hacker, Indonesian Journal of Criminal Law and Criminology (IJCLC)
- Arjaman Tatang & Akhmad Dede. 2019. Pendekatan Penelitian Kombinasi: Sebagai "Jalan Tengah" Atas Dikotomi Kuantitatif-Kualitatif, Jurnal Moderat, ISSN: 2442-3777 (cetak) Website: <https://jurnal.unigal.ac.id/index.php/moderat> ISSN: 2622-691X (online)
- Aziz Moh. Abdul, Kusriani & Asro Nasir. 2023. Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Domain Align Plan And Organize Studi Kasus: Akademi Komunitas Darussalam Blokagung Banyuwangi, TEKNIMEDIA
- Chazar Chalifa. 2015. Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005, , Jurnal Informasi
- Darwis Dedi & Yuniarwati. 2016. Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 4.1 Sebagai Upaya Peningkatan Keamanan Data Pada Dinas Pendidikan Dan Kebudayaan Kabupaten Pesawaran. Jurnal Sistem Informasi dan Telematika ISSN 2087-2062
- Dodo Zaenal Abidin. 2015. Kejahatan Dalam Teknologi Informasi Dan Komunikasi, Jurnal Ilmiah Media Processor
- Esther Indriana Limpeleh. 2023. Penerapan Pengendalian Internal Terkait Keamanan Sistem Informasi Akademik Hapzi, (2019). Sistem Informasi « sistem informasi. Sistem Informasi, 2, 2019. [https://d1wqtxts1xzle7.cloudfront.net/40023643/Bab\\_01\\_Data\\_dan\\_Informasi.pdf?1447602912=&response-contentdisposition=inline%3B+filename%3DBab\\_01\\_Data\\_dan\\_Informasi.pdf&Expires=1605595367&Signature=NB261yhnEnDNU5SxKhyNp--V4DBSM7bABubBEONhCBHfvTuyJXC8~0Uk](https://d1wqtxts1xzle7.cloudfront.net/40023643/Bab_01_Data_dan_Informasi.pdf?1447602912=&response-contentdisposition=inline%3B+filename%3DBab_01_Data_dan_Informasi.pdf&Expires=1605595367&Signature=NB261yhnEnDNU5SxKhyNp--V4DBSM7bABubBEONhCBHfvTuyJXC8~0Uk)
- Hoshmand Omer Mohammad & Ratnawati Suci. 2023. Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. AICOMS, Applied Information Technology and Computer Science (AICOMS)
- Idris Iswandi & Delvika Yuana. 2014. Analisis Perancangan Sistem Informasi Terintegrasi Di Lingkungan Perguruan Tinggi Swasta Di Medan, Jurnal Teknovasi 15 – 26 ISSN : 2355-701X 15
- Lipursari Anastasia. 2013. Peran Sistem Informasi Manajemen (Sim) Dalam Pengambilan Keputusan, Jurnal Stie Semarang (ISSN : 2252-7826)
- Ndrayani Etin. 2011. Pengelolaan Sistem Informasi Akademik Perguruan Tinggi Berbasis Teknologi Informasi Dan Komunikasi, Jurnal Penelitian Pendidikan

- 
- Matin Malik Muhamad Iik, Arini, Wardhani Kesuma Luh. 2017. JURNAL TEKNIK INFORMATIKA VOL.10 NO.2
- Muhammad Saleh, Ismail Yusuf & Herry Sujaini. 2021. Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas. JEPIN (Jurnal Edukasi dan Penelitian Informatika) ISSN(e): 2548-9364 / ISSN(p) : 2460-0741
- Murdiyanto Eko. 2020. Penelitian Kualitatif (Teori dan Aplikasi disertai contoh proposal), Lembaga Penelitian dan Pengabdian Pada Masyarakat UPN "Veteran" Yogyakarta Press
- M Adie Saputra & M Reza Redo. 2021. Penerapan Framework Cobit 2019 Untuk Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi. Journal of Science and Social Research ISSN 2615 – 4307 (Print) Oct 2021, IV (3): 352 – 364 ISSN 2615 – 3262 (Online) Available online at <http://jurnal.goretanpena.com/index.php/JSSR>
- Prasetyo Dwi. 2007. Pengembangan Sistem Informasi Geografis Tindak Kejahatan M (/L Tilo Vni Nnpj, Asts We B (Stiidi Kasus: Keltiratian Tanah Baru Bocor).
- Pratiwindya & Astari Retnowardhani. 2022. Penilaian Tata Kelola Teknologi Informasi Pada Institusi Pendidikan Tinggi Menggunakan Cobit 2019. STRING (Satuan Tulisan Riset dan Inovasi Teknologi) p - ISSN: 2527-9661 e-ISSN: 2549 -2837
- Rahmawati Ineu, 2017. Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense, Jurnal Pertahanan & Bela Negara
- Saputra Nur Dani & Herdiati Dian, 2020. Penerapan Flipped Classroom Pada Pembelajaran Teori Musik Di Prodi Pendidikan Musik, Pedagogia Jurnal Ilmu) <http://ejournal.upi.edu/index.php/pedagogia>
- Sepis Tomi Yeremia. 2022. Analisa Keamanan Sistem Informasi Menggunakan Framework Cobit 5 Dengan Domain Dss05 Dan Apo13di Pt Xyz, Jurnal TeIKa
- Shiddiq Susilo, Sistem Informasi Akademik Dan Administrasi Sdit Ar-Raihan Bantul, Teknik Iformasi
- Sinaga Fristia Meily, 2021. Analisis Sistem Dan Pengembangan Sistem Informasi Penerimaan Siswa Baru Tingkat SMA Berbasis Web Online Dengan Metode Kualitatif, SAINTEK (Jurnal Sains dan Teknologi) E - ISSN : 2714-8661
- Umara Rusydi, Riadib Imam, Handoyoc Eko, 2019. Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI), Jurnal Sistem Informasi Bisnis 01(2019) On-line : <http://ejournal.undip.ac.id/index.php/jsinbis>.