

**ANALISIS TINGKAT KEMATANGAN KEAMANAN LAYANAN
JARINGAN MENGGUNAKAN *FRAMEWORK* COBIT 2019
DENGAN *MATURITY LEVEL***

**Skripsi
untuk memenuhi Sebagian persyaratan
mencapai derajat Sarjana S-1 Program Studi
Teknik Komputer**



**DIMAS ADI KURNIAWAN
1903010003**

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS SAINS, TEKNOLOGI DAN PENDIDIKAN
UNIVERSITAS MUHAMMADIYAH LAMONGAN
2023**

HALAMAN PENGESAHAN

SKRIPSI

Analisis Tingkat Kematangan Keamanan Layanan Jaringan Menggunakan *Framework Cobit 2019 Dengan Maturity Level*

Oleh:

DIMAS ADI KURNIAWAN

1903010003

Telah diujikan dan dinyatakan lulus ujian skripsi pada tanggal 14 Agustus 2023 oleh tim penguji Program Studi Teknik Komputer Fakultas Sains, Teknologi, dan Pendidikan Universitas Muhammadiyah Lamongan.

Lamongan, 14 Agustus 2023

Mengetahui,

Pembimbing I



Mala Rosa Aprillya, S.Kom., M.Kom
NIDN. 701049502

Penguji



Bagus Dwi Saputra, S.Kom., M.Kom
NIDN. 0724099402

Pembimbing II




Eko Handoyo, S.Kom., M.Kom
NIDN. 0717029104

**Ketua Program Studi
Teknik Komputer**



Mufti Ari Bianto, S.Kom., M.Kom
NIDN. 0710069501

Mengetahui,
**Dekan Fakultas Sains
Teknologi dan Pendidikan**



Eko Handoyo, S.Kom., M.Kom
NIDN. 0717029104

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini :

Nama : Dimas Adi Kurniawan
NIM : 1903010003
Program Studi : Teknik Komputer
Fakultas : Sains Teknologi dan Pendidikan
Judul : Analisis Tingkat Kematangan Keamanan Layanan Jaringan Menggunakan *Framework* Cobit 2019 Dengan *Maturity Level*.

Dengan ini menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar akademik di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Lamongan, 14 Agustus 2023

Yang membuat pernyataan,



Dimas Adi Kurniawan

NIM. 1903010003

PERNYATAAN PERSETUJUAN
PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademis Universitas Muhammadiyah Lamongan, saya yang bertanda tangan di bawah ini :

Nama : Dimas Adi Kurniawan
NIM : 1903010003
Program Studi : Teknik Komputer
Fakultas : Sains Teknologi dan Pendidikan
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Lamongan Hak bebas Royalti Noneksklusif atas karya ilmiah saya yang berjudul :

Analisis Tingkat Kematangan Keamanan Layanan Jaringan
Menggunakan *Framework* Cobit 2019 Dengan *Maturity Level*

Beserta perangkat yang ada. Dengan Hak bebas Royalti Noneksklusif ini Program Studi Teknik Komputer Fakultas Sains, Teknologi dan Pendidikan Universitas Muhammadiyah Lamongan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database) merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Lamongan, 14 Agustus 2023

Yang membuat pernyataan,



Dimas Adi Kurniawan

NIM. 1903010003

KATA PENGANTAR

Alhamdulillah dengan puji syukur kepada Allah SWT, yang senantiasa melimpahkan rahmat serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Tingkat Kematangan Keamanan Layanan Jaringan Menggunakan *Framework* COBIT 2019 Dengan *Maturity Level*”

Pada kesempatan kali ini, penulis ingin menyampaikan ucapan terima kasih kepada seluruh pihak yang turut membantu dalam penyusunan skripsi ini, terutama kepada:

1. Eko Handoyo, S.Kom,. M.Kom selaku Dekan Fakultas Sains, Teknologi dan Pendidikan Universitas Muhammadiyah Lamongan.
2. Mufti Ari Bianto, S.Kom,. M.Kom selaku Ketua Program Studi Teknik Komputer Universitas Muhammadiyah Lamongan.
3. Mala Rosa Aprillya, S.Kom,. M.Kom selaku Dosen Pembimbing I Skripsi yang telah banyak membantu meluangkan waktu, perhatian, memberikan pengarahan dan masukan-masukan dalam penyusunan skripsi ini.
4. Eko Handoyo, S.Kom,. M.Kom selaku Dosen Pembimbing II yang telah memberikan pengarahan, dan masukan-masukan dalam penyusunan skripsi ini.
5. Kedua Orang Tua yang selalu memberikan dukungan materi, doa yang tulus selama penulisan skripsi dalam menyelesaikan pendidikan strata satu (S1). Terima kasih atas semua pengorbanan , perhatian dan kasih sayang yang diberikan selama ini.
6. Teruntuk Fika Faila Rosita yang selalu memberikan semangat, support, perhatian serta banyak membantu dalam penyusunan Skripsi ini. Terima kasih selalu menemani, meluangkan waktunya dalam keadaan apapun.
7. Seluruh pihak yang tidak dapat disebutkan satu per satu yang telah banyak membantu dalam pelaksanaan dan penyusunan Skripsi.

Terima kasih kepada semua pihak yang membantu dalam penyusunan skripsi sehingga penyusunan skripsi ini dapat terselesaikan dengan baik dan semoga Allah SWT memberikan balasannya. Penulis juga menerima segala kritik dan saran yang membangun dari semua pihak, karena penulis sadar akan keterbatasan dan kekurangan dalam skripsi ini. Penulis berharap semoga skripsi ini dapat bermanfaat serta dapat menambah pengetahuan bagi pembaca dan pihak yang memerlukan sebagaimana mestinya.

Penyusun

Dimas Adi Kurniawan

DAFTAR ISI

| | Halaman |
|--|---------|
| Halaman Judul..... | i |
| Halaman Pengesahan | ii |
| Halaman Pernyataan..... | iii |
| Halaman Pernyataan Publikasi..... | iv |
| Kata Pengantar | v |
| Daftar Isi..... | vii |
| Daftar Gambar..... | ix |
| Daftar Tabel | x |
| Daftar Lampiran | xi |
| Abstrak | xii |
| Abstrack | xiii |
| | |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Batasan Masalah..... | 3 |
| 1.4 Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian | 4 |
| | |
| BAB II TINJAUAN PUSTAKA DAN DASAR TEORI..... | 5 |
| 2.1 Tinjauan Pustaka | 5 |
| 2.2 Dasar Teori..... | 7 |
| 2.1.1 Teknologi Informasi..... | 7 |
| 2.1.2 Jaringan | 8 |
| 2.1.3 Keamanan Jaringan | 9 |
| 2.1.4 COBIT 2019..... | 10 |
| | |
| BAB III METODE PENELITIAN..... | 18 |
| 3.1 Bahan dan Alat Penelitian..... | 18 |
| 3.1.1 Bahan Penelitian..... | 18 |
| 3.1.2 Alat Penelitian | 18 |
| 3.2 Prosedur Penelitian..... | 18 |
| 3.3 Alur Penelitian | 19 |
| | |
| BAB IV HASIL PENELITIAN DAN PEMBAHASAN | 30 |
| 4.1 Hasil Penelitian | 30 |
| 4.2 Pembahasan..... | 44 |
| 4.2.1 Validasi DSS05 Dengan Aspek Keamanan | 44 |

| | Halaman |
|-----------------------------------|---------|
| 4.2.2 Hasil Pengolahan Data | 45 |
| 4.2.3 Rekomendasi | 48 |
| | |
| BAB V PENUTUP..... | 50 |
| 5.1 Kesimpulan | 50 |
| 5.2 Saran..... | 50 |
| | |
| DAFTAR PUSTAKA | 52 |
| LAMPIRAN | 56 |

DAFTAR GAMBAR

| | Halaman |
|--|---------|
| Gambar 2.1 COBIT 2019 | 11 |
| Gambar 2.2 Domain DSS COBIT 2019..... | 15 |
| Gambar 2.3 Skala <i>Maturity Level</i> | 16 |
| Gambar 3.1 Alur Penelitian..... | 19 |
| Gambar 4.1 GAP <i>Maturity Level</i> | 47 |

DAFTAR TABEL

| | Halaman |
|--|---------|
| Tabel 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan..... | 21 |
| Tabel 3.2 Kuesioner Pengguna (Dosen dan Mahasiswa)..... | 25 |
| Tabel 4.1 Switch Jaringan, Access Point Jaringan, Server Jaringan..... | 31 |
| Tabel 4.2 Penilaian Kuesioner | 33 |
| Tabel 4.3 Hasil Penilaian Kuesioner DSS05.01..... | 33 |
| Tabel 4.4 Hasil Penilaian Kuesioner DSS05.02..... | 35 |
| Tabel 4.5 Hasil Penilaian Kuesioner DSS05.03..... | 37 |
| Tabel 4.6 Hasil Penilaian Kuesioner DSS05.04..... | 38 |
| Tabel 4.7 Hasil Penilaian Kuesioner DSS05.05..... | 40 |
| Tabel 4.8 Hasil Penilaian Kuesioner DSS05.06..... | 41 |
| Tabel 4.9 Hasil Penilaian Kuesioner DSS05.07..... | 43 |
| Tabel 4.10 Aspek Keamanan | 45 |
| Tabel 4.11 Nilai kriteria <i>Maturity Level</i> | 45 |
| Tabel 4.12 Perhitungan maturity level..... | 45 |
| Tabel 4.13 Hasil Indeks / <i>Maturity Level</i> | 46 |
| Tabel 4.14 Maturity Level Sub Domain DSS05 | 47 |

DAFTAR LAMPIRAN

Halaman

| | |
|--|----|
| Lampiran 1 Penyebaran Kuesioner Kepada Responden | 56 |
|--|----|

ANALISIS TINGKAT KEMATANGAN KEAMANAN LAYANAN JARINGAN MENGGUNAKAN *FRAMEWORK* COBIT 2019 DENGAN *MATURITY LEVEL*

ABSTRAK

Penelitian ini dilatarbelakangi untuk menganalisis tingkat kematangan keamanan layanan jaringan menggunakan *framework COBIT* 2019 dengan *maturity level*. Penelitian ini dilakukan untuk mengetahui sejauh mana tingkat kematangan keamanan layanan jaringan menggunakan *framework* COBIT 2019 domain DSS05 dengan tujuan mengetahui kualitas keamanan layanan jaringan serta mengetahui tingkat kematangan keamanan jaringan menggunakan *framework* COBIT 2019 dengan *maturity level* di Universitas Muhammadiyah Lamongan. Metode penelitian yang digunakan adalah deskriptif kuantitatif dengan pendekatan COBIT 2019 domain DSS05 sub domain DSS05.01 sampai dengan sub domain DSS05.07 menggunakan *maturity level*. Hasil penelitian ini kualitas keamanan layanan jaringan yang ada di Universitas Muhammadiyah Lamongan 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 Universitas Muhammadiyah Lamongan sangat baik telah diukur berdasarkan sub domain DSS05 sub domain DSS05.01 hasil indeks 3,67 pada level 4, DSS05.02 hasil indeks 3,6 pada level 3, DSS05.03 hasil indeks 3,64 pada level 4, DSS05.04 hasil indeks 3,55 pada level 4, DSS05.05 hasil indeks 3,38 pada level 3, DSS05.06 hasil indeks 3,22 pada level 3, dan DSS05.07 hasil indeks 3,47 pada level 3.

Keyword: kematangan, keamanan, jaringan, COBIT, *maturity level*

ANALYSIS OF NETWORK SERVICE SECURITY Maturity LEVEL USING COBIT 2019 FRAMEWORK WITH MATURITY LEVEL

ABSTRACT

The background of this research is to analyze the maturity level of network service security using the COBIT 2019 framework with a maturity level. This research was conducted to determine the extent of network service security maturity level using the COBIT 2019 domain DSS05 framework with the aim of knowing the quality of network service security and knowing the level of network security maturity using the COBIT 2019 framework with maturity level at Muhammadiyah University Lamongan. The research method used is descriptive quantitative with the 2019 COBIT approach, the DSS05 domain, the DSS05.01 sub-domain to the DSS05.07 sub-domain, using a maturity level. The results of this study show that the quality of network service security at Muhammadiyah University of Lamongan has met the security standards measured regarding the DSS05 analysis in the 2019 COBIT framework with security parameters namely confidentiality, integrity and availability. The maturity level of network service security using the COBIT 2019 framework with a very good maturity level at Muhammadiyah University of Lamongan has been measured based on the DSS05 sub-domain, DSS05.01 sub-domain index result of 3.67 at level 4, DSS05.02 index result of 3.6 at level 3, DSS05.03 index result 3.64 at level 4, DSS05.04 index result 3.55 at level 4, DSS05.05 index result 3.38 at level 3, DSS05.06 index result 3.22 at level 3, and DSS05 .07 index result of 3.47 at level 3.

Keywords: *Maturity, security, network, COBIT, maturity level*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi saat ini semakin berkembang di semua kalangan bidang, seiring dengan bertambahnya kebutuhan fungsional organisasi untuk mencapai tujuan (Putra, 2022). Dalam instansi pemerintah penggunaan Teknologi Informasi sangatlah penting dalam menunjang efektivitas pelayanan publik sehingga sangat dibutuhkan pengetahuan serta sumber daya yang efisien (Agoan, 2017). Keseimbangan antara tujuan manajemen dengan pemanfaatan teknologi informasi yang sesuai dengan visi, misi, dan tujuan maupun strategi bisnis harus diperhatikan. Tata Kelola TI adalah cara untuk melakukan penyempurnaan tata kelola perusahaan ataupun organisasi yang menggunakan TI sebagai sarana penunjang untuk mempertahankan dan memperluas strategi dan tujuan bisnis (Surendro, 2009).

Di dalam suatu perusahaan atau organisasi Tata Kelola TI mencakup tentang kepemimpinan, struktur serta proses yang berkembang di dalamnya. Dalam Pemerintahan bahkan penggunaan TI dan transaksi elektronik, diatur dalam undang – undang, maka dari itu penggunaan TI dalam instansi perlu dilakukan analisa tingkat kematangan untuk *assessment* atau tinjauan diri dalam mengetahui kondisi TI dan organisasi serta internal (Boar, 2012), untuk mengetahui sejauh mana manfaat dari penggunaan TI dalam instansi.

Dalam penggunaan teknologi informasi sangat erat berkaitan dengan jaringan. Jaringan merupakan salah satu unit terpenting yang ada di dalam teknologi informasi, jaringan dan akses internet yang dikelola terdiri dari berbagai macam karakteristik *user* atau lebih dikenal pengguna jaringan. Jaringan internet saat ini telah digunakan dari berbagai kalangan anak-anak, remaja, hingga dewasa, bahkan sampai orang tua semua telah menggunakan internet baik untuk jejaring sosial, pencarian informasi, maupun kebutuhan lainnya yang berkaitan dengan internet (Nurcahyo, 2020).

Pada sebuah survei yang diselenggarakan Asosiasi Penyelenggara Jasa Internet Indonesia (APJSII) menyatakan bahwa jumlah pengguna internet di Indonesia tahun 2012 mencapai 63 juta orang atau 24,23 % dari total populasi negeri ini pada tahun 2013 meningkat 13 persen menjadi 71,19 juta orang, dan pada 2014 mencapai 107 juta orang yang menggunakan internet (Bobanto, 2014). Sehingga tidak bisa dipungkiri lagi bahwa internet adalah salah satu kebutuhan bagi semua orang.

Kualitas layanan internet yang diberikan oleh suatu *Internet Service Provider* (ISP) harus bagus untuk memberi pelayanan internet kepada para pengguna fasilitas internet (Bobanto, 2014). Salah satu pengguna *Internet Service Provider* (ISP) adalah Universitas Muhammadiyah Lamongan. Bagi suatu instansi yang bergerak pada bidang Pendidikan yang di dalamnya tidak jauh dari jaringan internet harus memberikan jasa layanan internet yang baik kepada para pengguna ataupun mahasiswa adalah suatu keharusan. Jaringan internet yang diberikan harus diperhatikan dan memadai dengan pengguna yang ada, sebab jika tidak memadai dengan pengguna akan menjadi kendala tersendiri dan menimbulkan masalah.

Untuk mencapai tujuan tersebut perlu dilakukan evaluasi agar dapat mengukur dan mengetahui sejauh mana level instansi tersebut dengan menggunakan suatu kerangka kerja (*framework*) COBIT 2019. COBIT (*Control Objectives for Information and Related Technology*), merupakan salah satu standar penting dan efektif untuk diterapkan.

Berdasarkan sedikit uraian di atas dengan ini pengkaji mengambil judul penelitian “Analisis Tingkat Kematangan Layanan Jaringan Menggunakan *Framework* COBIT 2019 Dengan *Maturity Level*”. Sehingga penelitian ini diharapkan dapat mengetahui tingkat kematangan keamanan layanan jaringan yang ada di Universitas Muhammadiyah Lamongan berada pada skala dan target yang telah ditentukan.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, maka dapat dirumuskan permasalahan sebagai berikut.

1. Bagaimana kualitas keamanan layanan jaringan yang ada pada Universitas Muhammadiyah Lamongan ?
2. Bagaimana mengetahui tingkat kematangan keamanan layanan jaringan menggunakan *framework* COBIT 2019 dengan *maturity level* di Universitas Muhammadiyah Lamongan ?

1.3 Batasan Masalah

Untuk menghindari agar tidak menyimpang dari permasalahan, maka penulis membatasi pembahasan ini, untuk proses-proses yang akan dibahas adalah sebagai berikut :

1. Lingkup dari penelitian ini dilakukan pada Universitas Muhammadiyah Lamongan bagian Teknologi Informasi.
2. Penelitian ini hanya menganalisis dengan menilai domain COBIT 2019 yaitu DSS05 (*Deliver, Support, and Service*)
3. Penilaian tingkat kematangan teknologi informasi menggunakan *Framework* COBIT 2019.
4. Penelitian ini menggunakan skala *Likert*.
5. Penelitian ini hanya menganalisis tingkat kematangan saat ini dan memberikan tahap rekomendasi.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut tujuan dari penelitian ini adalah :

1. Mengetahui kualitas keamanan layanan jaringan yang ada pada Universitas Muhammadiyah Lamongan.

2. Mengetahui tingkat kematangan keamanan jaringan menggunakan *framework* COBIT 2019 dengan *maturity level* di Universitas Muhammadiyah Lamongan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat, baik secara teoretis maupun praktis. Adapun manfaat teoretis dan manfaat praktis dipaparkan sebagaimana berikut ini :

1. Manfaat Teoretis

Hasil dari penelitian ini diharapkan dapat berguna dalam pengembangan ilmu teknologi khususnya dalam bidang jaringan internet. Penelitian ini diharapkan dapat memberikan tambahan ilmu pengetahuan mengenai tingkat kematangan jaringan menggunakan *framework* COBIT 2019.

2. Manfaat Praktis

- a. Bagi Pembaca

Hasil penelitian ini diharapkan memberikan kontribusi kepada pembaca mengenai pemahaman terhadap jaringan, terutama tingkat kematangan jaringan menggunakan *framework* COBIT 2019.

- b. Bagi Peneliti lain

Hasil penelitian ini diharapkan dapat memberikan inspirasi maupun bahan acuan peneliti lain untuk melakukan penelitian yang lebih mendalam terkait tingkat kematangan jaringan.

BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Penelitian dengan judul “Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019 (Studi Kasus Pada Rumah Sakit Bhayangkara Sespima Polri Jakarta) . Berdasarkan analisis tersebut dapat disimpulkan bahwa rumah sakit merupakan fasilitas pelayanan kesehatan yang perlu didukung oleh sistem informasi rumah sakit (SIM-RS) yang aman. Penelitian ini menggunakan COBIT 2019 sebagai *framework* penilaian. Penilaian pada penelitian ini mengacu kepada proses EDM03, APO12, APO13, APO14, dan DSS05. Hasil dari penelitian ini menunjukkan level kapabilitas tata kelola di RS Bhayangkara Sespima Polri Jakarta ini berada ditingkat 3 (Defined) (Gusni, 2021).

Penelitian yang dilakukan oleh Satriya Dwi Putra dengan judul “Evaluasi Tata Kelola Layanan Jaringan Menggunakan COBIT 2019 Pada Sekolah Tinggi Ilmu Kesehatan”. Tujuan penelitian yaitu mengukur tingkat kematangan pada layanan jaringan institusi yang berfokus pada *domain Delivery, Service, and Support* (DSS) *framework* COBIT 2019. Hasil pengukuran *maturity level* DSS02 memperoleh nilai 3,06 dan DSS05 memperoleh nilai 2,90 sehingga disimpulkan berada pada level 3 (Putra, 2022)

“Pengukuran Tingkat Kematangan Layanan TI Pada UPT Perpustakaan Universitas Sriwijaya Menggunakan *Framework* COBIT 2019”. Berdasarkan analisis tersebut dapat disimpulkan bahwa Penggunaan teknologi informasi di perpustakaan bertujuan untuk memastikan kemudahan akses, meningkatkan efisiensi kerja, meningkatkan kualitas layanan serta kemudahan dan kecepatan dalam memperoleh informasi. Berdasarkan pengukuran layanan TI yang telah dilakukan dengan melakukan analisis terhadap domain EDM04, APO11, dan DSS05, didapatkan hasil pengukuran tingkat *level* kematangan pada *domain* EDM04 berada pada *level* 2

(*Managed*), domain APO11 berada pada level 2 (*Managed*), dan domain DSS05 berada pada level 3 (*Defined*). Dikarenakan level yang diharapkan berada pada level 4 (*Quantitative*), maka terdapat *gap* yang terjadi sehingga perlu adanya rekomendasi perbaikan untuk dapat mengurangi *gap* dan mencapai level yang diharapkan (Aleksi, 2022).

Penelitian yang dilakukan oleh Muhammad Saleh dengan judul “Penerapan *Framework* COBIT 2019 Pada Audit Teknologi Informasi Di Politeknik Sambas”. Berdasarkan analisis dapat disimpulkan bahwa Teknologi informasi di suatu organisasi yang sudah berjalan harus diaudit agar diketahui kelebihan maupun kekurangannya. Berdasarkan hasil dari audit yang dilakukan pada teknologi informasi Poltesa, didapatkan rata-rata nilai sebesar 3,21 dengan nilai *maturity level* pada domain antara nilai 2 sampai dengan 4, yang berarti sistem telah dioperasikan dengan baik, akan tetapi belum secara maksimal (Saleh, 2021).

Penelitian yang dilakukan oleh Rizqi Agus Setiawan dengan judul “Evaluasi Tata Kelola dan Manajemen Teknologi Informasi Menggunakan *Framework* COBIT 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung Selatan”. Berdasarkan analisis dapat disimpulkan bahwa Kantor Dinas Komunikasi dan Informatika Kabupaten Lampung Selatan sebagai instansi pemerintahan yang berupaya untuk mengikuti perkembangan dalam menerapkan teknologi informasi (TI). Hasil dari penelitian ini adalah untuk nilai tingkat kemampuan pada DSS03 dan DSS05. Nilai *capability level* dan *maturity level* pada domain obyektif DSS 03 adalah 1,84 dengan persentase 36,90% dikategorikan *Partially*, sementara domain DSS 05 memperoleh nilai 2,57 dengan persentase 51,50% dan masuk kategori *Largely*. Hasil penelitian ini dapat merekomendasikan dan diimplementasikan untuk memperbaiki tata kelola TI Kantor Dinas Komunikasi dan Informatika Kabupaten Lampung Selatan (Setiawan, 2022).

2.2 Dasar Teori

2.1.1 Teknologi Informasi

Perkembangan teknologi berpengaruh terhadap dinamika sosial, budaya dan ekonomi masyarakat (Fitriani, 2018). Teknologi yang berhasil mendukung dinamika kehidupan masyarakat menjadi semakin baik, berkarakter dan kuat (Rahmawati, 2008). Diharapkan peningkatan ini mampu berkembang sesuai dengan kemajuan teknologi sehingga mendukung kemampuan intelektual masyarakat untuk berkompetisi dimasa depan. Membahas masalah teknologi berarti mengupas mengenai perkembangan dan kemajuan peradaban manusia. Semakin tinggi adab manusia maka semakin menunjang kemampuan untuk berkomunikasi dan bersosialisasi. Produk pendukung teknologi dan komunikasi pada saat ini berkembang dengan pesat dalam kehidupan masyarakat. Baik dalam menunjang kebutuhan pekerjaan maupun kebutuhan pribadi. Teknologi informasi merupakan istilah umum untuk seluruh teknologi yang mendukung manusia dalam membuat, mengubah, menyimpan, mengkomunikasikan dan atau menyebarkan informasi (Fitriani, 2018).

Kebutuhan akan informasi yang cepat, cakup dan akurat dalam kondisi lingkungan yang penuh dengan ketidakpastian mutlak diperlukan. Kebutuhan tersebut dapat dipenuhi jika perusahaan melakukan investasi dibidang teknologi informasi. Sabherwal dan King (1991); Grover dan Goslar (1993) membuktikan secara empiris bahwa teknologi informasi merupakan sarana untuk mengurangi ketidakpastian lingkungan organisasi (Rahmawati, 2008).

Investasi dibidang teknologi informasi dalam suatu organisasi sebagian besar bertujuan untuk dapat memberikan kontribusi yang positif terhadap kinerja individual anggota organisasi dan institusiya. Teknologi informasi khususnya teknologi komputer sangat berpotensi untuk memperbaiki performa individu dan organisasi, karenanya banyak pengambil keputusan menginvestasikan dana untuk teknologi informasi (Rahmawati, 2008).

Teknologi informasi meliputi teknologi komputer (*computing technology*) dan teknologi komunikasi (*communication technology*) yang digunakan untuk memproses dan menyebarkan informasi baik itu yang bersifat finansial atau non finansial (Bodnar dan Hopwood, 1995). Sehingga dapat dikatakan bahwa Teknologi informasi adalah segala cara atau alat yang terintegrasi yang digunakan untuk menjaring data, mengolah dan mengirimkan atau menyajikan secara elektronik menjadi informasi dalam berbagai format yang bermanfaat bagi pemakainya. (Ficher 1996 dalam Silvia, 2001) menyatakan bahwa manfaat teknologi informasi baru dapat dirasakan jika pengguna teknologi informasi tersebut “menyadari” manfaatnya. Disamping itu, perkembangan teknologi informasi yang sangat cepat dalam lingkungan kerja menyebabkan pemanfaatan teknologi informasi menjadi masalah yang mendesak (Rahmawati, 2008)..

Penggunaan teknologi informasi saat ini semakin berkembang di semua kalangan bidang, seiring dengan bertambahnya kebutuhan fungsional organisasi untuk mencapai tujuan (Putra, 2022). Dalam instansi pemerintah penggunaan Teknologi Informasi sangatlah penting dalam menunjang efektivitas pelayanan publik sehingga sangat dibutuhkan pengetahuan serta sumber daya yang efisien (Agoan, 2017). Keselarasan antara tujuan manajemen teknologi informasi yang sesuai visi, misi, dan tujuan serta strategi bisnis harus diperhatikan.

2.1.2 Jaringan

Dalam penggunaan teknologi informasi sangat erat berkaitan dengan jaringan. Jaringan merupakan salah satu unit terpenting yang ada di dalam teknologi informasi, jaringan dan akses internet yang dikelola terdiri dari berbagai macam karakteristik *user* atau lebih dikenal pengguna jaringan. Jaringan internet saat ini telah digunakan dari berbagai kalangan anak-anak, remaja, hingga dewasa, bahkan sampai orang tua semua telah menggunakan internet baik untuk jejaring sosial, pencarian informasi, maupun kebutuhan lainnya yang berkaitan dengan internet (Nurcahyo, 2020).

2.1.3 Keamanan Jaringan

Keamanan pada jaringan sangat diperlukan, sebab pengguna komputer sangat menyadari bahwa kenyamanan penggunaan komputer dalam kehidupan kita sehari-hari adalah hal yang paling dasar, karena fungsinya seperti otomatisasi, kedirgantaraan, kedokteran dan kesehatan, penelitian ilmiah, investigasi kriminal dan sebagainya, komputer memiliki peran penting yang tidak tergantikan. Terdapat banyak informasi dalam industri yang sifatnya sangat rahasia, karena ini informasi tidak dapat dipahami oleh orang yang tidak relevan, jika tidak maka akan menyebabkan kerugian yang tidak dapat diperbaiki (Munawar, 2020).

Tepatnya karena tingginya rahasia informasi komputer sehingga beberapa orang yang berniat jahat memiliki ide untuk melakukan kejahatan dan selalu berharap untuk mendapatkan beberapa manfaat dari kerentanan keamanan jaringan komputer. Jaringan komputer teknologi keamanan terus berkembang, dan teknologi kriminal dari para penjahat ini juga terus menerus berkembang. Ada hal penting yang perlu dilakukan yaitu melakukan pekerjaan dengan baik dalam pencegahan keamanan jaringan komputer, untuk meminimalkan kemungkinan terjadinya kejahatan komputer (Munawar, 2020).

Keamanan jaringan komputer tidak terdiri dari satu aspek, tetapi mengandung empat tautan penting: perangkat lunak, perangkat keras jaringan, layanan *Internet of Things* dan sumber daya bersama. Menurut definisi komputer keamanan jaringan oleh Organisasi Internasional untuk Standardisasi, keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah, atau lubang keamanan karena alasan kecelakaan atau berbahaya, sehingga sistem komputer terus beroperasi dengan handal, serta layanan komputer juga teratur (Munawar, 2020).

2.1.4 COBIT 2019

Control Objective for Information and related Technology (COBIT) merupakan kerangka kerja untuk tata kelola dan pengelolaan informasi dan teknologi perusahaan. Teknologi dan informasi perusahaan merujuk pada seluruh teknologi dan pemrosesan informasi yang diterapkan oleh perusahaan, tidak hanya oleh departemen teknologi dan informasi. Kerangka COBIT membagi antara kegiatan tata kelola dan manajemen (ISACA, 2018).

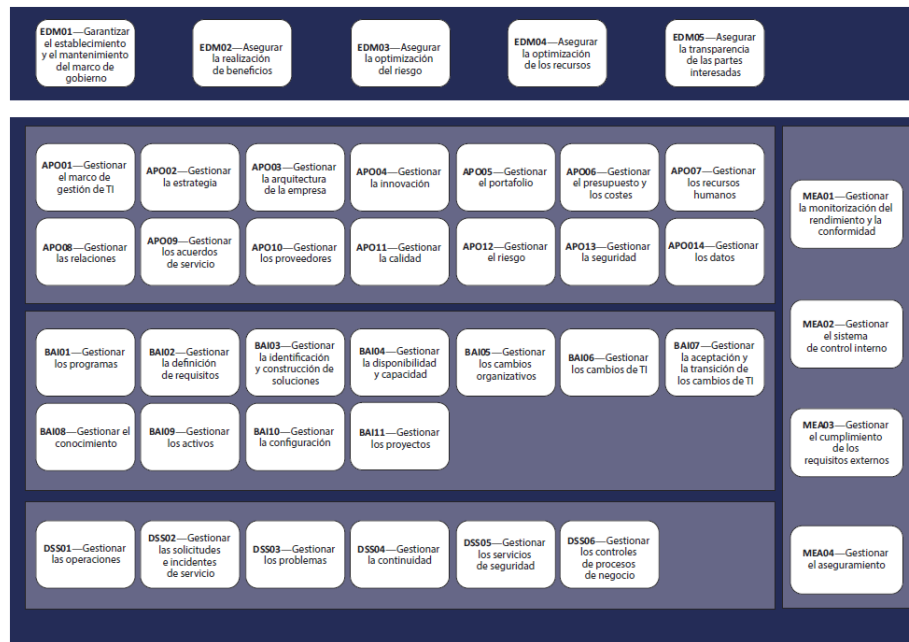
Menurut COBIT, tata kelola meliputi kegiatan memastikan bahwa kebutuhan, kondisi dan pilihan stakeholder dievaluasi untuk menentukan tujuan bisnis yang sesuai, memastikan arahan ditetapkan dengan cara memerhatikan prioritas dan pengambilan keputusan, serta memastikan kinerja dan kepatuhan setiap elemen perusahaan dipantau berdasarkan tujuan yang telah disepakati. Sedangkan, manajemen meliputi kegiatan merencanakan, membangun, menjalankan dan memantau aktivitas yang dilaksanakan sesuai dengan arahan yang ditetapkan oleh tata kelola guna mencapai tujuan perusahaan (ISACA, 2018).

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 (ISACA, 2018) :

1. COBIT 2019 *Framework* : Pengenalan dan metodologi. Menjelaskan tentang konsep kunci dari COBIT 2019.
2. COBIT 2019 *Framework* : Objektif tata kelola dan manajemen. Menjelaskan tentang 40 inti tujuan tata kelola dan manajemen, proses yang ada, serta komponen lain.
3. COBIT 2019 *Design Guide* : Merancang solusi tata kelola teknologi dan informasi. Menjelaskan desain faktor yang dapat memengaruhi tata kelola dan mencakup alur kerja untuk merancang sistem tata kelola yang disesuaikan untuk perusahaan.

4. COBIT 2019 *Implementation Guide* : Menerapkan dan mengoptimalkan solusi tata kelola teknologi dan informasi.

Perubahan dari panduan penerapan COBIT 5 dan pengembangan *road map* untuk perbaikan tata kelola yang berkelanjutan, seperti ditunjukkan gambar 2.1.



Gambar 2.1 COBIT 2019

A. Prinsip COBIT 2019

COBIT 2019 memiliki dua prinsip yaitu prinsip yang menjelaskan kebutuhan inti dari sistem tata kelola bagi perusahaan teknologi dan informasi dan prinsip sebagai kerangka tata kelola yang dapat digunakan untuk membangun sistem tata kelola bagi perusahaan. Berikut merupakan prinsip COBIT 2019 sebagai sistem tata kelola bagi perusahaan teknologi dan informasi:

1. Perusahaan membutuhkan sistem tata kelola untuk memenuhi kebutuhan stakeholder dan menghasilkan nilai atau manfaat dari penggunaan teknologi dan informasi.
2. Sistem tata kelola untuk perusahaan TI dibangun dari beberapa komponen dari berbagai jenis dan bekerja sama secara holistik.

3. Sistem tata kelola harus dinamis seiring dengan perubahan desain faktor.
4. Sistem tata kelola harus dengan jelas membedakan antara tata kelola dengan struktur dan aktivitas manajemen.
5. Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan menggunakan rangkaian design factor sebagai parameternya.
6. Sistem tata kelola harus mencakup keseluruhan perusahaan.

Berikut merupakan prinsip COBIT 2019 sebagai kerangka tata yang dapat digunakan untuk membangun sistem tata kelola bagi perusahaan :

1. Kerangka tata kelola harus berdasar pada model konseptual, mengidentifikasi komponen utama dan hubungan antar komponen tersebut, serta dapat memaksimalkan optimalisasi dan memberikan kemungkinan. otomatisasi
2. Kerangka tata kelola harus memungkinkan fleksibilitas dan keterbukaan.
3. Kerangka tata kelola dapat menyelaraskan standard, kerangka kerja dan regulasi utama yang sesuai.

B. Domain COBIT 2019

COBIT 2019 membagi fokus tujuan menjadi dua yaitu tujuan tata kelola dan manajemen. Dari tujuan ini dibagi menjadi lima *domain*. Dalam tujuan tata kelola, dikelompokkan dalam domain yang bernama *Evaluate, Direct and Monitor* (EDM) yang memiliki 5 *core model*. Domain EDM membahas struktur tata kelola melakukan evaluasi pilihan strategis, mengarahkan manajemen senior dalam memutuskan pilihan strategis dan mengawasi setiap pencapaian strategi. Dalam tujuan manajemen, dikelompokkan dalam empat domain yaitu (ISACA, 2018) :

1. *Align, Plan, and Organize* (APO) membahas keseluruhan organisasi, strategi, dan kegiatan pendukung. Terdapat 14 *core model* dalam domain APO.
2. *Build, Acquire and Implement* (BAI) membahas definisi ancaman, hasil, dan implementasi teknologi dan informasi serta memastikan keselarasan antara solusi

teknologi dan informasi dengan proses bisnis. Terdapat 11 *core model* dalam domain BAI.

3. *Monitor, Evaluate, and Assess* (MEA) membahas terkait pemantauan kinerja dan kesesuaian teknologi dan informasi dengan target, tujuan internal dan kebutuhan eksternal. Terdapat 4 *core model* dalam domain MEA.
4. *Deliver, Service, and Support* (DSS) membahas pengiriman operasional teknologi informasi serta layanan pendukungnya. Terdapat 7 *core model* dalam domain DSS.

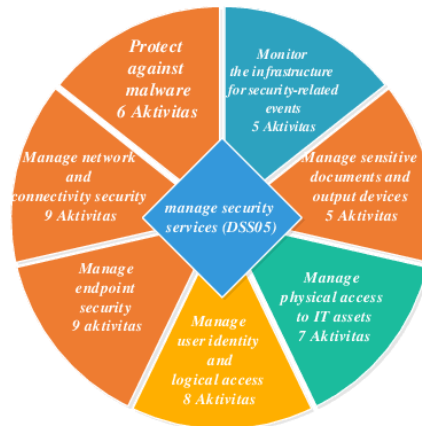
C. *Deliver, Service, and Support* (DSS05)

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 Sub-domain

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) digunakan 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*) (missal: 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 devisi 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, seperti ditunjukkan pada gambar 2.2.



Gambar 2.2 Domain DSS COBIT 2019

D. Teori Pemingkatan

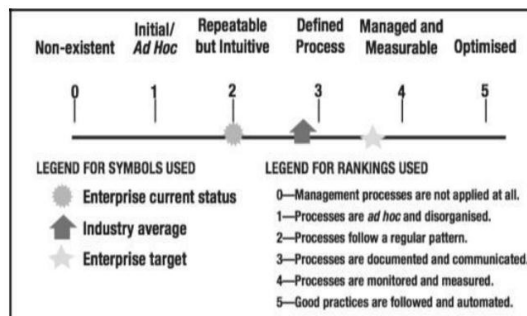
Menurut (CMMI Product Team, 2010) Model CMMI menempatkan insitusi dalam 5 *Maturity Level* atau tingkat kematangan dalam CMMI yaitu :

1. Level 1: *Initial* atau proses Awal. Kondisi ini institusi yang berapa pada level ini adalah institusi yang belum menjalankan CMMI.
2. Level 2: *Managed* atau Dikelola. Institusi memiliki beberapa proses yang sering digunakan dalam setiap proyek pengembangan, akan tetapi tidak terdapat keseragaman secara menyeluruh.
3. Level 3: *Defined* atau Ditetapkan. Institusi telah menjalankan proses yang sudah didefinisikan dan semua tim paham bagaimana proses seharusnya berjalan.
4. Level 4: *Quantitatively Managed* atau Dikelola secara kuantitatif. Institusi semakin terstruktur dan terbuka dengan sistem yang ada. Mereka mulai menerapkan konsep kuantifikasi pada setiap proses, dan selalu dimonitoring serta dikontrol dalam setiap proses kerjanya.
5. Level 5: *Optimizing* atau Mengoptimalkan. *Level* ini adalah *level* puncak dalam model CMMI. Pada *Maturity Level* 5 ini suatu institusi sudah mencapai seluruh spesifik dan generik *goals* yang ada di *Level* 2, 3, 4, dan 5. Fokus kepada peningkatan proses secara berkesinambungan melalui inovasi teknologi dan

optimasi proses senantiasa dimonitoring dan dianalisis. Sehingga mampu memberikan sistem yang optimal.

E. *Maturity Level*

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 dan organisasi 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 2.3.



Gambar 2.3 *Skala Maturity Level*

Berdasarkan gambar 2.3, 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: Ditetapkan (*Defined process*): Tahap dimana manajemen telah berhasil menciptakan dan mengkomunikasikan standar buku pengelolaan proses terkait walaupun belum dilakukan secara terintegrasi.
5. Level 4: Dikelola (*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: Mengoptimalkan (*Optimised*): Tahap dimana manajemen telah berkomitmen terhadap proses yang ada agar dapat menjadi sebuah *best practice* yang selalu dikembangkan.

BAB III

METODE PENELITIAN

3.1 Bahan dan Alat Penelitian

3.1.1 Bahan Penelitian

Bahan penelitian yang akan digunakan oleh penulis mencakup hasil survey dan observasi yang telah dilakukan. Bahan-bahan tersebut antara lain :

- a. Data jaringan Universitas Muhammadiyah Lamongan
- b. Data keamanan layanan jaringan Universitas Muhammadiyah Lamongan

3.1.2 Alat Penelitian

Dalam penelitian ini, penulis menggunakan alat penelitian berupa :

- a. Kuesioner
- b. Wawancara kepada pihak-pihak yang terkait (kepala IT, Staff IT)
- c. Framework COBIT 2019

3.2 Prosedur Penelitian

Pada penelitian ini, prosedur pengumpulan informasi yang digunakan sebagai bahan penelitian dilakukan dengan dua cara yaitu :

- a. Kuesioner

Kuesioner dilakukan langsung kepada pihak-pihak yang terlibat untuk mengetahui bagaimana tingkat kualitas jaringan yang terdapat di Universitas Muhammadiyah Lamongan, pengambilan data menggunakan metode kuesioner dengan cara pengambilan data yang terdiri dari pertanyaan-pertanyaan ditujukan kepada narasumber. Proses kuesioner ini bertujuan untuk mendapatkan informasi melalui pertanyaan-pertanyaan yang diajukan oleh pewawancara kepada narasumber yang diwawancarai.

Dalam tahap ini, dilakukan kuesioner kepada kepala pimpinan TI Universitas Muhammadiyah Lamongan untuk mengetahui permasalahan yang sedang dihadapi oleh TI Universitas Muhammadiyah Lamongan terkait dengan tingkat kualitas

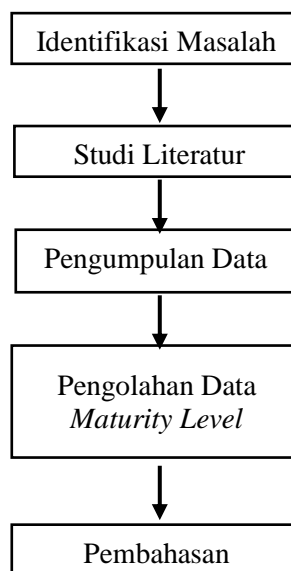
jaringan maupun keamanan layanan jaringan di Universitas Muhammadiyah Lamongan.

b. Wawancara

Wawancara dilakukan untuk memperoleh informasi berupa tanya jawab dengan responden sebagai pendukung hasil kuesioner. Wawancara digunakan untuk mendapatkan informasi lebih lengkap mengenai masalah yang diteliti yang tidak ada pada kuesioner.

3.3 Alur Penelitian

Untuk mengetahui tingkat kematangan keamanan layanan jaringan, penulis menggunakan metode Analisis Deskriptif kuantitatif. Metode Analisis Deskriptif kuantitatif digunakan pada penelitian ini untuk mengetahui serta menjelaskan hasil kuesioner yang telah disebar. Metode ini dianggap sebagai metode yang tepat karena harus menjelaskan dan menganalisis dari hasil data yang diperoleh, seperti gambar 3.1.



Gambar 3.1 Alur Penelitian

Kerangka berpikir digunakan untuk menjelaskan pola antar teori dan objek dalam penelitian. Pemikiran dimulai dari latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian. Di bawah ini penjelasan alur penelitian :

A. Identifikasi Masalah

Identifikasi masalah dilakukan untuk mencari atau mengetahui kualitas keamanan layanan jaringan, kemudian mencari bagaimanakah tingkat kematangan layanan jaringan yang akan dijadikan objek penelitian menggunakan *framework* COBIT 2019 Domain DSS05.

B. Studi Literatur

Studi literatur dilakukan dengan cara mencari rujukan sumber data berupa jurnal-jurnal, artikel, buku-buku ataupun sumber relevan lainnya yang berkaitan dengan objek penelitian.

C. Pengumpulan Data

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.

D. 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.

E. Pembahasan

Di dalam 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 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan dan tabel 3.2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa).

Tabel 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan

| 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 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan (lanjutan)

| DSS05.02 Mengelola keamanan jaringan dan konektivitas | | | | | | |
|--|--|----------|----------|----------|----------|----------|
| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
| 6. | Menerapkan mekanisme penyaringan jaringan, seperti firewall dan perangkat lunak pendeteksi intrusi. | | | | | |
| 7. | Merapkan kebijakan yang sesuai untuk mengontrol lalu lintas jaringan masuk dan keluar. | | | | | |
| 8. | Menerapkan protokol keamanan yang disetujui ke konektivitas jaringan. | | | | | |
| 9. | Mengkon figurasikan peralatan jaringan dengan cara yang aman. | | | | | |
| 10. | Berdasarkan penilaian risiko dan persyaratan bisnis, membuat dan mempertahankan kebijakan untuk keamanan konektivitas. | | | | | |
| DSS05.03 Kelola keamanan titik akhir | | | | | | |
| 11. | Mewujudkan sistem operasi dengan cara yang aman. | | | | | |
| 12. | Menerapkan mekanisme penguncian perangkat. | | | | | |
| 13. | Mengelola akses dan kontrol jarak jauh seperti perangkat seluler. | | | | | |
| 14. | Mengelola struktur jaringan dengan cara yang aman. | | | | | |
| 15. | Selalu melindungi integritas sistem. | | | | | |
| DSS05.04 Kelola identitas pengguna dan akses logis | | | | | | |
| 16. | Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses, dan kebijakan keamanan. | | | | | |

Tabel 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|---|
| 17. | Menyelaraskan pengelolaan identitas dan hak akses ke peran dan tanggung jawab yang ditentukan, berdasarkan prinsip-prinsip yang paling tidak diistimewakan, perlu dimiliki dan perlu diketahui. | | | | | |
| 18. | Memastikan semua akses ke aset informasi berdasarkan peran individu atau aturan bisnis. | | | | | |
| 19. | Berkoordinasi dengan unit bisnis yang mengelola autentikasi dalam aplikasi yang digunakan dalam proses bisnis untuk memastikan bahwa kontrol autentikasi telah dikelola dengan benar. | | | | | |
| 20. | Melakukan tinjauan manajemen secara teratur terhadap semua akun dan hak istimewa terkait. | | | | | |
| DSS05.05 Mengelola akses fisik ke asset I&T | | | | | | |
| 21. | Memastikan semua anggota menampilkan identifikasi yang disetujui dengan benar setiap saat. | | | | | |
| 22. | Mematasi dan memantau akses ke situs TI sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan perangkat keamanan di pintu interior dan eksterior. | | | | | |
| 23. | Mengelola permintaan untuk mengizinkan akses resmi yang sesuai ke fasilitas komputasi. | | | | | |
| 24. | Memastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area, atau zona) berdasarkan fungsi dan tanggung jawab pekerjaan. | | | | | |

Tabel 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|---|
| DSS05.06 Kelola dokumen sensitive dan perangkat keluaran | | | | | | |
| 25. | Melakukan pelatihan kesadaran keamanan informasi fisik secara teratur. | | | | | |
| 26. | Menetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan, dan pemusnahan dokumen sensitif dan perangkat keluaran ke dalam, di dalam, dan di luar perusahaan. | | | | | |
| 27. | Memastikan kontrol kriptografi tersedia untuk melindungi informasi sensitif yang disimpan secara elektronik. | | | | | |
| 28. | Membuat inventarisasi dokumen sensitif dan perangkat keluaran, dan lakukan rekonsiliasi rutin. | | | | | |
| 29. | Menetapkan pengamanan fisik yang sesuai atas dokumen sensitif. | | | | | |
| 30. | Menerapkan kontrol kriptografi untuk memastikan perlindungan informasi sensitif (kerahasiaan, keaslian, integritas). | | | | | |
| DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan | | | | | | |
| 31. | Selalu menggunakan portofolio teknologi, layanan, dan aset yang didukung (seperti pemindai kerentanan, fuzzers dan sniffer, penganalisa protokol) untuk mengidentifikasi kerentanan keamanan informasi. | | | | | |
| 32. | Menentukan dan mengkomunikasikan skenario risiko sehingga dapat dengan mudah dikenali dan kemungkinan serta dampaknya dipahami. | | | | | |

Tabel 3.1 Kuesioner Pihak IT Universitas Muhammadiyah Lamongan (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|---|
| DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan | | | | | | |
| 33. | Meninjau log peristiwa secara teratur untuk potensi insiden keamanan. | | | | | |
| 34. | Memastikan tiket insiden terkait keamanan dibuat tepat waktu saat pemantauan mengidentifikasi potensi insiden keamanan. | | | | | |
| 35. | Mencatat peristiwa terkait keamanan dan menyimpan catatan untuk periode yang sesuai. | | | | | |

Keterangan :

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

Tabel 3.2 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 3.2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa) (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|---|
| DSS05.01 Melindungi dari perangkat lunak berbahaya | | | | | | |
| 4. | Menyebarkan informasi semua perangkat lunak untuk perlindungan secara terpusat. | | | | | |
| 5. | Memberikan tinjauan informasi secara berkala tentang potensi ancaman baru (misalnya, meninjau saran keamanan produk). | | | | | |
| DSS05.02 Mengelola keamanan jaringan dan konektivitas | | | | | | |
| 6. | Menjalankan mekanisme pemilihan jaringan, seperti perangkat lunak pendeteksi intrusi untuk keamanan. | | | | | |
| 7. | Diterapkan kebijakan yang sesuai untuk mengontrol jalannya jaringan masuk dan keluar. | | | | | |
| 8. | Sudah diterapkannya protokol keamanan yang disetujui ke konektivitas jaringan. | | | | | |
| 9. | Membentuk peralatan jaringan dengan cara yang aman. | | | | | |
| 10. | Telah membuat dan mempertahankan kebijakan untuk keamanan konektivitas. | | | | | |
| DSS05.03 Kelola keamanan titik akhir | | | | | | |
| 11. | Selalu mewujudkan sistem operasi perangkat dengan cara yang aman. | | | | | |
| 12. | Telah menggunakan autentikasi dua faktor dan enkripsi termasuk mekanisme penguncian perangkat. | | | | | |
| 13. | Telah melakukan paengelolaan akses dan kontrol jarak jauh seperti perangkat seluler. | | | | | |
| 14. | Mengelola struktur jaringan dengan cara yang aman. | | | | | |
| 15. | Selalu melindungi integritas sistem. | | | | | |

Tabel 3.2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa) (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| DSS05.04 Kelola identitas pengguna dan akses logis | | | | | | |
| 16. | Menjaga hak akses pengguna sesuai dengan fungsi kebijakan keamanan. | | | | | |
| 17. | Telah menyelaraskan pengelolaan identitas dan hak akses ke pengguna berdasarkan tanggung jawab yang ditentukan. | | | | | |
| 18. | Selalu memastikan semua akses ke aset informasi termasuk peran individu atau aturan bisnis. | | | | | |
| 19. | Mengelola autentikasi dalam aplikasi yang digunakan untuk memastikan bahwa kontrol autentikasi telah dikelola dengan benar. | | | | | |
| 20. | Telah melakukan tinjauan manajemen secara teratur terhadap semua akun. | | | | | |
| DSS05.05 Mengelola akses fisik ke asset I&T | | | | | | |
| 21. | Menampilkan identifikasi yang disetujui dengan benar untuk semua anggota. | | | | | |
| 22. | Telah dilakukan pembatasan dan memantau akses ke situs dengan menetapkan batasan perimeter, seperti pagar, dinding, dan perangkat keamanan di pintu interior dan eksterior. | | | | | |
| 23. | Adanya perizinan untuk akses resmi yang sesuai ke fasilitas komputasi. | | | | | |
| 24. | Selalu memastikan akses profil tetap terkini. | | | | | |
| 25. | Adanya pelatihan kesadaran keamanan informasi fisik secara rutin. | | | | | |

Tabel 3.2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa) (lanjutan)

| DSS05.06 Kelola dokumen sensitive dan perangkat keluaran | | | | | | |
|--|--|----------|----------|----------|----------|----------|
| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
| 26. | Menetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan, dan pemusnahan dokumen sensitif dan perangkat arn ke dalam, di dalam, dan di luar perusahaan. | | | | | |
| 27. | Memastikan kontrol kriptografi tersedia untuk melindungi informasi sensitif yang disimpan secara elektronik. | | | | | |
| 28. | Membuat inventarisasi dokumen sensitif dan perangkat keluaran, dan lakukan rekonsiliasi rutin. | | | | | |
| 29. | Menetapkan pengamanan fisik yang sesuai atas dokumen sensitif. | | | | | |
| 30. | Menerapkan kontrol kriptografi untuk memastikan perlindungan informasi sensitif (kerahasiaan, keaslian, integritas). | | | | | |
| DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan | | | | | | |
| 31. | Telah menggunakan portofolio teknologi, layanan, dan aset yang didukung untuk mengidentifikasi kerentanan keamanan informasi. | | | | | |
| 32. | Telah meninjau daftar peristiwa secara teratur untuk potensi kejadian keamanan. | | | | | |
| 33. | Adanya penetapan skenario risiko sehingga dapat dengan mudah dikenali dan kemungkinan serta dampaknya dipahami. | | | | | |
| 34. | Memastikan terkait keamanan yang telah dibuat tepat waktu saat pemantauan mengidentifikasi potensi kejadian keamanan. | | | | | |

Tabel 3.2 Kuesioner Untuk Pengguna (Dosen dan Mahasiswa) (lanjutan)

| No | Pernyataan | 1 | 2 | 3 | 4 | 5 |
|--|--|---|---|---|---|---|
| DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan | | | | | | |
| 35. | Telah dilakukan pencatatan peristiwa terkait keamanan dan menyimpan catatan untuk periode yang sesuai. | | | | | |

Keterangan :

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

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

A Hasil Wawancara

1. Visi dan Misi UPT ICT

Pengembangan Universitas Muhammadiyah Lamongan 2019 – 2024 mengarah kepada peningkatan layanan dalam bidang Teknologi Informasi dan pengembangan *world class university* dengan berbagai macam layanan berbasis teknologi informasi.

- a. Pemantapan Infrastruktur Teknologi Informasi
- b. Meningkatkan layanan dalam bidang akademik berbasis teknologi informasi (*cybercampus*)
- c. Meningkatkan layanan fasilitas penunjang proses belajar mengajar dengan menggunakan *e-learning*.
- d. Meningkatkan layanan fasilitas *email*, *blog*, dan *hosting* untuk civitas akademik.
- e. Memberikan lulusan Universitas Muhammadiyah Lamongan yang terbaik dengan pembekalan dalam bidang teknologi informasi melalui seminar, kursus.
- f. Mengadakan kerjasama dengan vendor teknologi informasi seperti *Google*, *Microsoft*, *Cisco* dan *vendor* lainnya yang terkait dengan teknologi informasi.

Switch Jaringan yaitu komponen jaringan yang memiliki fungsi berhubungan ke beberapa perangkat komputer dalam beberapa jaringan. Tahapan ini membuat pengguna bertukar data dan informasi ke perangkat yang diinginkan. Kemudian *Acces Point* berfungsi sebagai penghasil sinyal internet, selain itu juga berfungsi sebagai pengaturan konektivitas yang menyeluruh. Selain itu *Server* Jaringan

merupakan perangkat yang berguna menyalurkan sambungan kabel ke *nirkabel*, seperti pada tabel 4.1.

Tabel 4.1 Switch Jaringan, Acces Point, Server Jaringan Universitas Muhammadiyah Lamongan

| SWITCH JARINGAN | | | | | |
|--|----------------------------|---------------------------------|------------------|---------------|------------|
| UNIVERSITAS MUHAMMADIYAH LAMONGAN | | | | | |
| No | Merek | Spesifikasi | Kecepatan | Jumlah | KET |
| 1 | TPLINK | 16 PORT | 10/100MBps | 5 | Baik |
| 2 | CISCO | 24 PORT | 10/100/1000MBps | 1 | Baik |
| 3 | CISCO | 8 PORT | 10/100MBps | 8 | Baik |
| 4 | DLINK | 8 PORT | 10/100MBps | 6 | Baik |
| 5 | TPLINK | 8 PORT | 10/100MBps | 5 | Baik |
| 6 | HP | 24 PORT | 10/100/1000MBps | 1 | Baik |
| ACCES POINT JARINGAN | | | | | |
| UNIVERSITAS MUHAMMADIYAH LAMONGAN | | | | | |
| No | Merek | SPEKIFIKASI | KECEPATAN | JUMLAH | KET |
| 1 | Ruijie AP 720 L | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 5 | Baik |
| 2 | Ruijie AP 720 L | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 1 | Rusak |
| 3 | ZTE ZGHN F460 | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 4 | Baik |
| 4 | ZTE ZGHN F460 | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 1 | Rusak |
| 5 | TPLINK WA701ND | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 2 | Baik |
| 6 | TPLINK Archer C5400X | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000MBps | 2 | Baik |

Tabel 4.1 Switch Jaringan, Acces Point, Server Jaringan Universitas Muhammadiyah Lamongan (lanjutan)

| 7 | NETGEAR Nighthawk XR500X | A/B/G/N/AC (2,4GHz/ 5GHz) | 10/100/1000Mbps | 1 | Baik |
|--|--------------------------------|---|-----------------|--------|-----------------------|
| SERVER JARINGAN | | | | | |
| UNIVERSITAS MUHAMMADIYAH LAMONGAN | | | | | |
| NO | MEREK | SPESIFIKASI | | JUMLAH | KETERANGAN |
| 1 | HP ML 110 GEN 9 | <i>Intel® Xeon® E5-2603v4 (1.7GHz/6-core/15MB/85W), 8GB (1 x 8GB) PC4-2400-R DDR4 RDIMM, Dual-port 1Gb, B140i, 1TB SATA, DVDRW, 5xPCI-E, 350W,</i> | | 2 | BAIK |
| 2 | ASUS TS100-E9- PI4 | <i>Socket LGA1151 for Intel® Xeon® E3-1200 v6/v5 processors High energy-efficiency and stability Complete server management with ASUS Control Center (ACC) Flexible and convenient connectivity Built-in dual Intel® I210 server- class Gigabit LAN USB 3.0 for high-speed external</i> | | 2 | ASUS TS100- E9-PI4 |
| 3 | DELL R630 | <i>Intel® Xeon® E5-2603v4 (1.7GHz/6-core/15MB/85W), 32GB (4 x 8GB) PC4-2400-R DDR4 RDIMM, Four-port LAN 1Gb, One-port LAN 10Gb, B140i, 1TB SATA, DVDRW, 2xPCI-E, 350W,</i> | | 1 | Baik |

2. IT Backbone

Kebutuhan akan akses informasi tidak dapat dihindari lagi satu sama lain diharapkan dapat berkomunikasi dengan baik, sebagai contoh mahasiswa dapat mengakses informasi perkuliahan, layanan akademik, informasi status pembayaran dan kegiatan lainnya yang akan selalu menggunakan teknologi

informasi. Universitas Muhammadiyah Lamongan dituntut untuk dapat melayani seluruh civitas akademik maupun non civitas akademik. Kebutuhan pembangunan IT *backbone* sebagai tulang punggung jaringan komputer mutlak diperlukan dan benar-benar bagus karena tanpa *backbone* maka seluruh komunikasi baik internal maupun eksternal dapat terganggu.

B Hasil Kuesioner

Dari kuesioner yang telah disebarakan dimana sesuai dengan standar *framework* COBIT 2019 dan diberikan penilaian dengan skala *likert* dimana dalam kuesioner ini terdapat 5 penilaian seperti pada Tabel 4.2.

Tabel 4.2 Penilaian Kuesioner

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

Dari penilaian kuesioner pada Tabel 4.2, 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 4.3.

Tabel 4.3 Hasil Penilaian Kuesioner DSS05.01

| Responden | DSS05.01 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 5 | 25 |
| 2 | 5 | 5 | 5 | 5 | 5 | 25 |
| 3 | 5 | 5 | 5 | 5 | 5 | 25 |

Tabel 4.3 Hasil Penilaian Kuesioner DSS05.01 (lanjutan)

| Responden | DSS05.01 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 4 | 4 | 4 | 4 | 3 | 4 | 19 |
| 5 | 2 | 3 | 2 | 2 | 4 | 13 |
| 6 | 3 | 2 | 1 | 1 | 2 | 9 |
| 7 | 2 | 3 | 3 | 3 | 3 | 14 |
| 8 | 2 | 3 | 3 | 2 | 4 | 14 |
| 9 | 4 | 3 | 3 | 4 | 3 | 17 |
| 10 | 4 | 4 | 3 | 4 | 4 | 19 |
| 11 | 4 | 4 | 4 | 4 | 4 | 20 |
| 12 | 4 | 5 | 5 | 5 | 5 | 24 |
| 13 | 4 | 3 | 4 | 2 | 4 | 17 |
| 14 | 3 | 3 | 3 | 3 | 3 | 15 |
| 15 | 4 | 4 | 4 | 4 | 5 | 21 |
| 16 | 4 | 3 | 5 | 3 | 4 | 19 |
| 17 | 5 | 5 | 4 | 5 | 5 | 24 |
| 18 | 4 | 3 | 4 | 4 | 4 | 19 |
| 19 | 4 | 3 | 3 | 5 | 4 | 19 |
| 20 | 4 | 4 | 5 | 3 | 4 | 20 |
| 21 | 1 | 2 | 3 | 4 | 5 | 15 |
| 22 | 3 | 4 | 5 | 5 | 5 | 22 |
| 23 | 5 | 5 | 4 | 4 | 3 | 21 |
| 24 | 4 | 3 | 4 | 4 | 4 | 19 |
| 25 | 5 | 3 | 5 | 4 | 4 | 21 |
| 26 | 4 | 5 | 4 | 4 | 5 | 22 |
| 27 | 4 | 3 | 4 | 4 | 4 | 19 |
| 28 | 5 | 3 | 4 | 4 | 4 | 20 |
| 29 | 1 | 2 | 2 | 1 | 2 | 8 |
| 30 | 3 | 2 | 2 | 3 | 2 | 12 |
| 31 | 2 | 2 | 3 | 3 | 2 | 12 |
| 32 | 5 | 4 | 4 | 4 | 4 | 21 |
| 33 | 4 | 4 | 5 | 5 | 5 | 23 |
| 34 | 5 | 4 | 4 | 5 | 5 | 23 |
| 35 | 3 | 4 | 2 | 1 | 1 | 11 |
| 36 | 4 | 4 | 3 | 3 | 2 | 16 |
| 37 | 5 | 4 | 4 | 3 | 4 | 20 |
| 38 | 4 | 4 | 3 | 5 | 5 | 21 |
| 39 | 4 | 4 | 4 | 3 | 1 | 16 |
| 40 | 4 | 3 | 2 | 2 | 2 | 13 |
| 41 | 5 | 5 | 4 | 4 | 3 | 21 |

Tabel 4.3 Hasil Penilaian Kuesioner DSS05.01 (lanjutan)

| Responden | DSS05.01 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 42 | 4 | 4 | 3 | 2 | 2 | 15 |
| 43 | 5 | 4 | 4 | 5 | 3 | 21 |
| 44 | 5 | 5 | 4 | 4 | 3 | 21 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| TOTAL DSS05.01 | | | | | | 826 |

Dari Tabel 4.3 dapat disimpulkan bahwa sub domain DSS05.01 Melindungi dari perangkat lunak berbahaya dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 9 dan presentase sebanyak 20% , Setuju dengan frekuensi 19 dan presentase 42%, Ragu-ragu dengan frekuensi 10 dan presentase 22%, Tidak setuju dengan frekuensi 5 dan presentase 11%, Sangat tidak setuju dengan frekuensi 2 dan presentase 4%.

Tabel 4.4 Hasil Penilaian Kuesioner DSS05.02

| Responden | DSS05.02 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 5 | 25 |
| 2 | 5 | 5 | 5 | 5 | 5 | 25 |
| 3 | 5 | 5 | 5 | 5 | 5 | 25 |
| 4 | 2 | 3 | 1 | 2 | 2 | 10 |
| 5 | 3 | 2 | 2 | 3 | 3 | 13 |
| 6 | 2 | 3 | 2 | 3 | 3 | 13 |
| 7 | 3 | 2 | 2 | 4 | 4 | 15 |
| 8 | 1 | 1 | 2 | 3 | 2 | 9 |
| 9 | 3 | 2 | 3 | 4 | 2 | 14 |
| 10 | 3 | 3 | 2 | 5 | 3 | 16 |
| 11 | 5 | 5 | 4 | 4 | 5 | 23 |
| 12 | 5 | 4 | 4 | 5 | 5 | 23 |
| 13 | 4 | 3 | 4 | 4 | 4 | 19 |
| 14 | 5 | 4 | 5 | 4 | 5 | 23 |
| 15 | 4 | 4 | 5 | 5 | 4 | 22 |
| 16 | 5 | 5 | 4 | 4 | 4 | 22 |
| 17 | 3 | 4 | 3 | 4 | 4 | 18 |
| 18 | 4 | 4 | 3 | 4 | 4 | 19 |
| 19 | 4 | 3 | 5 | 4 | 4 | 20 |
| 20 | 4 | 4 | 5 | 5 | 4 | 22 |
| 21 | 1 | 2 | 3 | 4 | 5 | 15 |

Tabel 4.4 Hasil Penilaian Kuesioner DSS05.02 (lanjutan)

| Responden | DSS05.02 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 22 | 3 | 5 | 5 | 5 | 4 | 22 |
| 23 | 4 | 4 | 4 | 3 | 3 | 18 |
| 24 | 4 | 5 | 4 | 4 | 4 | 21 |
| 25 | 4 | 4 | 3 | 2 | 4 | 17 |
| 26 | 5 | 4 | 5 | 4 | 5 | 23 |
| 27 | 4 | 5 | 4 | 4 | 4 | 21 |
| 28 | 4 | 4 | 5 | 4 | 4 | 21 |
| 29 | 1 | 1 | 2 | 1 | 2 | 7 |
| 30 | 2 | 2 | 2 | 2 | 2 | 10 |
| 31 | 3 | 4 | 3 | 3 | 2 | 15 |
| 32 | 4 | 4 | 4 | 4 | 5 | 21 |
| 33 | 4 | 3 | 4 | 4 | 4 | 19 |
| 34 | 4 | 4 | 4 | 4 | 4 | 20 |
| 35 | 2 | 3 | 3 | 3 | 3 | 14 |
| 36 | 3 | 3 | 3 | 4 | 2 | 15 |
| 37 | 4 | 3 | 4 | 4 | 2 | 17 |
| 38 | 3 | 4 | 3 | 2 | 4 | 16 |
| 39 | 2 | 2 | 3 | 4 | 4 | 15 |
| 40 | 2 | 3 | 3 | 4 | 5 | 17 |
| 41 | 4 | 4 | 3 | 2 | 5 | 18 |
| 42 | 3 | 3 | 4 | 2 | 4 | 16 |
| 43 | 4 | 4 | 3 | 5 | 4 | 20 |
| 44 | 4 | 4 | 3 | 4 | 5 | 20 |
| 45 | 3 | 3 | 3 | 4 | 3 | 16 |
| TOTAL DSS05.02 | | | | | | 810 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.02 Mengelola keamanan jaringan dan konektivitas dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 11 dan presentase sebanyak 24% , Setuju dengan frekuensi 14 dan presentase 31%, Ragu-ragu dengan frekuensi 14 dan presentase 31%, Tidak setuju dengan frekuensi 4 dan presentase 8%, Sangat tidak setuju dengan frekuensi 2 dan presentase 4%.

Tabel 4.5 Hasil Penilaian Kuesioner DSS05.03

| Responden | DSS05.03 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 5 | 25 |
| 2 | 5 | 5 | 5 | 5 | 5 | 25 |
| 3 | 5 | 5 | 5 | 5 | 5 | 25 |
| 4 | 3 | 2 | 3 | 4 | 2 | 14 |
| 5 | 4 | 2 | 3 | 3 | 3 | 15 |
| 6 | 2 | 3 | 2 | 2 | 3 | 12 |
| 7 | 3 | 1 | 1 | 4 | 2 | 11 |
| 8 | 1 | 2 | 3 | 2 | 3 | 11 |
| 9 | 2 | 3 | 3 | 4 | 5 | 17 |
| 10 | 5 | 4 | 4 | 5 | 3 | 21 |
| 11 | 5 | 5 | 5 | 5 | 5 | 25 |
| 12 | 5 | 4 | 4 | 4 | 4 | 21 |
| 13 | 3 | 4 | 4 | 4 | 4 | 19 |
| 14 | 4 | 5 | 4 | 5 | 3 | 21 |
| 15 | 4 | 5 | 2 | 4 | 5 | 20 |
| 16 | 5 | 3 | 4 | 5 | 4 | 21 |
| 17 | 4 | 4 | 4 | 4 | 4 | 20 |
| 18 | 4 | 3 | 3 | 4 | 5 | 19 |
| 19 | 4 | 4 | 3 | 5 | 5 | 21 |
| 20 | 4 | 4 | 5 | 4 | 3 | 20 |
| 21 | 4 | 3 | 2 | 1 | 2 | 12 |
| 22 | 4 | 5 | 3 | 4 | 5 | 21 |
| 23 | 5 | 5 | 4 | 3 | 4 | 21 |
| 24 | 4 | 5 | 4 | 4 | 4 | 21 |
| 25 | 3 | 4 | 3 | 3 | 3 | 16 |
| 26 | 4 | 5 | 5 | 4 | 5 | 23 |
| 27 | 5 | 3 | 4 | 4 | 4 | 20 |
| 28 | 5 | 3 | 3 | 4 | 5 | 20 |
| 29 | 1 | 2 | 2 | 2 | 2 | 9 |
| 30 | 2 | 2 | 2 | 3 | 2 | 11 |
| 31 | 4 | 2 | 3 | 2 | 2 | 13 |
| 32 | 5 | 5 | 4 | 4 | 4 | 22 |
| 33 | 4 | 5 | 5 | 5 | 4 | 23 |
| 34 | 4 | 5 | 4 | 4 | 4 | 21 |
| 35 | 4 | 2 | 2 | 4 | 4 | 16 |
| 36 | 2 | 2 | 3 | 4 | 2 | 13 |
| 37 | 4 | 3 | 2 | 4 | 1 | 14 |
| 38 | 3 | 3 | 3 | 5 | 5 | 19 |

Tabel 4.5 Hasil Penilaian Kuesioner DSS05.03 (lanjutan)

| Responden | DSS05.03 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 39 | 4 | 3 | 3 | 2 | 5 | 17 |
| 40 | 5 | 3 | 3 | 5 | 5 | 21 |
| 41 | 5 | 3 | 4 | 5 | 5 | 22 |
| 42 | 4 | 3 | 2 | 3 | 1 | 13 |
| 43 | 4 | 3 | 3 | 4 | 2 | 16 |
| 44 | 5 | 3 | 4 | 3 | 3 | 18 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| TOTAL DSS05.03 | | | | | | 820 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.03 Kelola keamanan titik akhir dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 8 dan presentase sebanyak 17% , Setuju dengan frekuensi 19 dan presentase 42%, Ragu-ragu dengan frekuensi 9 dan presentase 20%, Tidak setuju dengan frekuensi 8 dan presentase 17%, Sangat tidak setuju dengan frekuensi 1 dan presentase 2%.

Tabel 4.6 Hasil Penilaian Kuesioner DSS05.04

| Responden | DSS05.04 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 5 | 25 |
| 2 | 5 | 5 | 5 | 5 | 5 | 25 |
| 3 | 5 | 5 | 5 | 5 | 5 | 25 |
| 4 | 2 | 3 | 3 | 3 | 2 | 13 |
| 5 | 4 | 3 | 1 | 3 | 3 | 14 |
| 6 | 3 | 3 | 3 | 2 | 4 | 15 |
| 7 | 2 | 3 | 1 | 4 | 3 | 13 |
| 8 | 4 | 3 | 3 | 2 | 1 | 13 |
| 9 | 5 | 3 | 4 | 2 | 3 | 17 |
| 10 | 5 | 4 | 4 | 3 | 4 | 20 |
| 11 | 4 | 4 | 5 | 5 | 4 | 22 |
| 12 | 5 | 4 | 4 | 5 | 4 | 22 |
| 13 | 5 | 5 | 5 | 3 | 4 | 22 |
| 14 | 4 | 5 | 3 | 4 | 5 | 21 |
| 15 | 3 | 4 | 3 | 4 | 4 | 18 |
| 16 | 5 | 4 | 5 | 4 | 5 | 23 |
| 17 | 5 | 4 | 4 | 5 | 4 | 22 |
| 18 | 4 | 4 | 3 | 4 | 4 | 19 |
| 19 | 4 | 4 | 5 | 3 | 4 | 20 |

Tabel 4.6 Hasil Penilaian Kuesioner DSS05.04 (lanjutan)

| Responden | DSS05.04 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 20 | 4 | 3 | 4 | 4 | 4 | 19 |
| 21 | 3 | 4 | 5 | 4 | 3 | 19 |
| 22 | 4 | 5 | 3 | 4 | 5 | 21 |
| 23 | 4 | 4 | 4 | 3 | 3 | 18 |
| 24 | 4 | 5 | 5 | 4 | 4 | 22 |
| 25 | 4 | 3 | 4 | 2 | 3 | 16 |
| 26 | 5 | 5 | 4 | 4 | 5 | 23 |
| 27 | 4 | 3 | 4 | 4 | 4 | 19 |
| 28 | 5 | 4 | 3 | 4 | 5 | 21 |
| 29 | 1 | 1 | 2 | 2 | 1 | 7 |
| 30 | 2 | 2 | 2 | 3 | 2 | 11 |
| 31 | 3 | 2 | 1 | 2 | 3 | 11 |
| 32 | 5 | 4 | 4 | 4 | 5 | 22 |
| 33 | 5 | 4 | 4 | 5 | 5 | 23 |
| 34 | 4 | 5 | 4 | 4 | 4 | 21 |
| 35 | 2 | 1 | 1 | 3 | 3 | 10 |
| 36 | 4 | 3 | 2 | 2 | 1 | 12 |
| 37 | 4 | 2 | 3 | 3 | 3 | 15 |
| 38 | 4 | 3 | 4 | 5 | 4 | 20 |
| 39 | 5 | 4 | 4 | 3 | 3 | 19 |
| 40 | 2 | 1 | 2 | 2 | 3 | 10 |
| 41 | 2 | 3 | 2 | 3 | 3 | 13 |
| 42 | 3 | 2 | 1 | 2 | 3 | 11 |
| 43 | 2 | 3 | 3 | 2 | 2 | 12 |
| 44 | 4 | 3 | 3 | 5 | 5 | 20 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| TOTAL DSS05.04 | | | | | | 799 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.04 Kelola identitas pengguna dan akses logis dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 12 dan presentase sebanyak 27% , Setuju dengan frekuensi 15 dan presentase 33%, Ragu-ragu dengan frekuensi 6 dan presentase 13%, Tidak setuju dengan frekuensi 11 dan presentase 24%, Sangat tidak setuju dengan frekuensi 1 dan presentase 2%.

Tabel 4.7 Hasil Penilaian Kuesioner DSS05.05

| Responden | DSS05.05 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 2 | 22 |
| 2 | 5 | 5 | 5 | 5 | 2 | 22 |
| 3 | 5 | 5 | 5 | 5 | 2 | 22 |
| 4 | 3 | 2 | 3 | 2 | 2 | 12 |
| 5 | 2 | 3 | 2 | 2 | 3 | 12 |
| 6 | 4 | 3 | 2 | 4 | 2 | 15 |
| 7 | 1 | 2 | 3 | 2 | 2 | 10 |
| 8 | 2 | 3 | 2 | 4 | 1 | 12 |
| 9 | 4 | 3 | 3 | 5 | 4 | 19 |
| 10 | 4 | 4 | 4 | 4 | 3 | 19 |
| 11 | 4 | 4 | 5 | 5 | 4 | 22 |
| 12 | 4 | 4 | 4 | 5 | 5 | 22 |
| 13 | 4 | 4 | 3 | 5 | 5 | 21 |
| 14 | 5 | 4 | 5 | 4 | 4 | 22 |
| 15 | 2 | 3 | 4 | 3 | 4 | 16 |
| 16 | 5 | 4 | 3 | 4 | 5 | 21 |
| 17 | 4 | 4 | 5 | 5 | 5 | 23 |
| 18 | 4 | 4 | 3 | 3 | 4 | 18 |
| 19 | 3 | 3 | 4 | 5 | 4 | 19 |
| 20 | 4 | 4 | 4 | 4 | 3 | 19 |
| 21 | 1 | 2 | 3 | 4 | 5 | 15 |
| 22 | 2 | 4 | 2 | 5 | 5 | 18 |
| 23 | 4 | 4 | 4 | 5 | 4 | 21 |
| 24 | 3 | 3 | 4 | 3 | 3 | 16 |
| 25 | 4 | 4 | 3 | 3 | 4 | 18 |
| 26 | 5 | 4 | 5 | 5 | 5 | 24 |
| 27 | 4 | 4 | 4 | 4 | 3 | 19 |
| 28 | 4 | 4 | 5 | 4 | 3 | 20 |
| 29 | 2 | 1 | 2 | 2 | 2 | 9 |
| 30 | 2 | 2 | 2 | 2 | 3 | 11 |
| 31 | 3 | 2 | 3 | 1 | 2 | 11 |
| 32 | 3 | 4 | 4 | 3 | 5 | 19 |
| 33 | 4 | 4 | 4 | 5 | 5 | 22 |
| 34 | 4 | 5 | 3 | 4 | 4 | 20 |
| 35 | 3 | 2 | 3 | 2 | 3 | 13 |
| 36 | 1 | 1 | 2 | 3 | 3 | 10 |
| 37 | 3 | 3 | 3 | 4 | 2 | 15 |
| 38 | 5 | 4 | 3 | 5 | 4 | 21 |

Tabel 4.7 Hasil Penilaian Kuesioner DSS05.05 (lanjutan)

| Responden | DSS05.05 | | | | | Jumlah |
|------------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 39 | 3 | 2 | 2 | 4 | 3 | 14 |
| 40 | 2 | 2 | 3 | 3 | 2 | 12 |
| 41 | 3 | 1 | 2 | 4 | 3 | 13 |
| 42 | 3 | 1 | 1 | 2 | 3 | 10 |
| 43 | 2 | 3 | 3 | 2 | 2 | 12 |
| 44 | 5 | 2 | 2 | 4 | 3 | 16 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| JUMLAH DSS05.05 | | | | | | 762 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.05 Mengelola akses fisik ke asset IT dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 9 dan presentase sebanyak 20% , Setuju dengan frekuensi 15 dan presentase 33%, Ragu-ragu dengan frekuensi 8 dan presentase 18%, Tidak setuju dengan frekuensi 12 dan presentase 26%, Sangat tidak setuju dengan frekuensi 1 dan presentase 2%.

Tabel 4.8 Hasil Penilaian Kuesioner DSS05.06

| Responden | DSS05.06 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 2 | 2 | 2 | 16 |
| 2 | 5 | 5 | 2 | 2 | 2 | 16 |
| 3 | 5 | 5 | 2 | 2 | 2 | 16 |
| 4 | 3 | 2 | 2 | 2 | 3 | 12 |
| 5 | 3 | 4 | 4 | 4 | 3 | 18 |
| 6 | 2 | 1 | 1 | 2 | 2 | 8 |
| 7 | 2 | 1 | 3 | 2 | 2 | 10 |
| 8 | 2 | 4 | 3 | 2 | 1 | 12 |
| 9 | 2 | 2 | 3 | 4 | 3 | 14 |
| 10 | 4 | 3 | 4 | 5 | 4 | 20 |
| 11 | 5 | 5 | 5 | 4 | 5 | 24 |
| 12 | 3 | 5 | 5 | 5 | 5 | 23 |
| 13 | 4 | 4 | 4 | 3 | 4 | 19 |
| 14 | 4 | 3 | 4 | 5 | 4 | 20 |
| 15 | 3 | 4 | 4 | 4 | 4 | 19 |
| 16 | 5 | 4 | 3 | 4 | 5 | 21 |
| 17 | 4 | 4 | 5 | 5 | 5 | 23 |
| 18 | 3 | 4 | 4 | 3 | 4 | 18 |
| 19 | 4 | 4 | 5 | 5 | 4 | 22 |

Tabel 4.8 Hasil Penilaian Kuesioner DSS05.06 (lanjutan)

| Responden | DSS05.06 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 20 | 4 | 3 | 4 | 5 | 4 | 20 |
| 21 | 4 | 3 | 2 | 1 | 2 | 12 |
| 22 | 1 | 3 | 4 | 5 | 5 | 18 |
| 23 | 4 | 5 | 5 | 4 | 4 | 22 |
| 24 | 4 | 3 | 4 | 5 | 5 | 21 |
| 25 | 4 | 4 | 4 | 4 | 4 | 20 |
| 26 | 5 | 5 | 5 | 5 | 5 | 25 |
| 27 | 4 | 4 | 3 | 4 | 4 | 19 |
| 28 | 5 | 4 | 3 | 5 | 4 | 21 |
| 29 | 1 | 2 | 2 | 2 | 3 | 10 |
| 30 | 2 | 2 | 2 | 2 | 2 | 10 |
| 31 | 3 | 1 | 2 | 3 | 2 | 11 |
| 32 | 4 | 5 | 4 | 5 | 5 | 23 |
| 33 | 4 | 4 | 5 | 4 | 4 | 21 |
| 34 | 4 | 5 | 4 | 4 | 5 | 22 |
| 35 | 2 | 1 | 1 | 2 | 3 | 9 |
| 36 | 3 | 2 | 1 | 1 | 2 | 9 |
| 37 | 2 | 3 | 4 | 2 | 1 | 12 |
| 38 | 3 | 3 | 2 | 1 | 1 | 10 |
| 39 | 3 | 3 | 2 | 4 | 3 | 15 |
| 40 | 1 | 2 | 1 | 1 | 2 | 7 |
| 41 | 1 | 1 | 4 | 4 | 3 | 13 |
| 42 | 3 | 3 | 3 | 4 | 1 | 14 |
| 43 | 1 | 1 | 3 | 2 | 2 | 9 |
| 44 | 2 | 1 | 1 | 1 | 1 | 6 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| TOTAL DSS05.06 | | | | | | 725 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.06 Kelola dokumen sensitive dan perangkat keluaran dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 8 dan presentase sebanyak 18% , Setuju dengan frekuensi 14 dan presentase 31%, Ragu-ragu dengan frekuensi 5 dan presentase 11%, Tidak setuju dengan frekuensi 10 dan presentase 22%, Sangat tidak setuju dengan frekuensi 6 dan presentase 13%.

Tabel 4.9 Hasil Penilaian Kuesioner DSS05.07

| Responden | DSS05.07 | | | | | Jumlah |
|-----------|----------|---|---|---|---|--------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 5 | 5 | 5 | 5 | 5 | 25 |
| 2 | 5 | 5 | 5 | 5 | 5 | 25 |
| 3 | 5 | 5 | 5 | 5 | 5 | 25 |
| 4 | 2 | 3 | 2 | 3 | 2 | 12 |
| 5 | 3 | 3 | 3 | 4 | 2 | 15 |
| 6 | 3 | 3 | 3 | 2 | 3 | 14 |
| 7 | 3 | 2 | 1 | 3 | 4 | 13 |
| 8 | 3 | 5 | 4 | 2 | 2 | 16 |
| 9 | 2 | 2 | 4 | 3 | 3 | 14 |
| 10 | 4 | 3 | 4 | 5 | 4 | 20 |
| 11 | 4 | 4 | 4 | 4 | 5 | 21 |
| 12 | 4 | 5 | 5 | 3 | 5 | 22 |
| 13 | 4 | 4 | 4 | 3 | 5 | 20 |
| 14 | 4 | 4 | 4 | 5 | 4 | 21 |
| 15 | 4 | 4 | 4 | 4 | 4 | 20 |
| 16 | 5 | 4 | 4 | 5 | 4 | 22 |
| 17 | 3 | 3 | 3 | 4 | 4 | 17 |
| 18 | 4 | 4 | 3 | 4 | 4 | 19 |
| 19 | 4 | 2 | 2 | 3 | 4 | 15 |
| 20 | 4 | 4 | 3 | 4 | 4 | 19 |
| 21 | 3 | 1 | 2 | 3 | 5 | 14 |
| 22 | 5 | 2 | 3 | 5 | 5 | 20 |
| 23 | 4 | 3 | 4 | 4 | 3 | 18 |
| 24 | 4 | 4 | 4 | 5 | 3 | 20 |
| 25 | 3 | 4 | 3 | 3 | 4 | 17 |
| 26 | 5 | 5 | 5 | 5 | 5 | 25 |
| 27 | 3 | 4 | 4 | 4 | 4 | 19 |
| 28 | 4 | 5 | 4 | 3 | 4 | 20 |
| 29 | 3 | 1 | 1 | 2 | 1 | 8 |
| 30 | 2 | 2 | 2 | 2 | 3 | 11 |
| 31 | 1 | 2 | 3 | 4 | 2 | 12 |
| 32 | 5 | 4 | 4 | 5 | 5 | 23 |
| 33 | 3 | 3 | 4 | 4 | 4 | 18 |
| 34 | 4 | 4 | 4 | 4 | 4 | 20 |
| 35 | 3 | 2 | 2 | 3 | 3 | 13 |
| 36 | 2 | 3 | 3 | 3 | 2 | 13 |
| 37 | 1 | 2 | 3 | 3 | 2 | 11 |
| 38 | 2 | 3 | 2 | 3 | 4 | 14 |

Tabel 4.9 Hasil Penilaian Kuesioner DSS05.07 (lanjutan)

| Responden | DSS05.07 | | | | | Jumlah |
|-----------------------|----------|---|---|---|---|------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 39 | 3 | 2 | 4 | 5 | 5 | 19 |
| 40 | 2 | 2 | 4 | 3 | 3 | 14 |
| 41 | 3 | 3 | 4 | 4 | 3 | 17 |
| 42 | 3 | 2 | 3 | 2 | 2 | 12 |
| 43 | 3 | 3 | 3 | 4 | 2 | 15 |
| 44 | 4 | 4 | 3 | 4 | 4 | 19 |
| 45 | 3 | 3 | 3 | 3 | 3 | 15 |
| TOTAL DSS05.07 | | | | | | 782 |

Dari tabel di atas dapat disimpulkan bahwa sub domain DSS05.07 Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan dengan kriteria jawaban yang di dapat Sangat Setuju frekuensi 7 dan presentase sebanyak 15% , Setuju dengan frekuensi 16 dan presentase 36%, Ragu-ragu dengan frekuensi 13 dan presentase 29%, Tidak setuju dengan frekuensi 8 dan presentase 18%, Sangat tidak setuju dengan frekuensi 1 dan presentase 2%.

4.2 Pembahasan

4.2.1 Validasi DSS05 Dengan Aspek Keamanan

Validasi ini merupakan analisis DSS05 pada *framework* COBIT 2019 dengan parameter keamanan yaitu Kerahasiaan (*Confidentiality*), Integritas (*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 integritas, 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 integritas dan ketersediaan, DSS05.06 kelola dokumen sensitive dan perangkat keluaran menyatakan bahwa validasi keamanan bersifat integritas, DSS05.07 kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan. Seperti pada Tabel di bawah ini :

Tabel 4.10 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 | | ✓ | |

4.2.2 Hasil Pengolahan Data

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 4.11 Nilai kriteria maturity level

| Level | Kriteria | Keterangan |
|-------|-------------|-------------------------------|
| 1 | 0,0 – 1,50 | <i>Initial</i> |
| 2 | 0,51 – 2,50 | <i>Managed and measurable</i> |
| 3 | 2,51 – 3,50 | <i>Defined process</i> |
| 4 | 3,51 – 4,50 | <i>Managed and measurable</i> |
| 5 | 4,51 – 5,00 | <i>Optimised</i> |

Hasil dari kuesioner yang telah di berikan terhadap responden dan telah di isi oleh responden di dapatkan hasil seperti pada Tabel 4.3. Selanjutnya akan dihitung *indeks* kematangan sebagai berikut :

Tabel 4.12 Perhitungan Maturity Level

| <i>Maturity Level</i> | | | | | | | | |
|-------------------------|------------------|----------|------------------|----------|-------------------------------------|----------|-----------------------|----------------------|
| Proses Sub Domain DSS05 | Total Pertanyaan | | Jumlah Responden | | Total Pernyataan x Jumlah Responden | | Total Nilai Kuesioner | Jumlah Nilai Jawaban |
| | IT | Pengguna | IT | Pengguna | IT | Pengguna | (IT+Pengguna) | |
| 01 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 826 |

Tabel 4.12 Perhitungan Maturity Level (lanjutan)

| | | | | | | | | |
|---|-------------|---|---|----|----|-----|------|-----|
| 02 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 810 |
| 03 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 820 |
| 04 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 799 |
| 05 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 762 |
| 06 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 725 |
| 07 | 5 | 5 | 3 | 42 | 15 | 210 | 225 | 782 |
| <i>Indeks Kematangan = (jumlah nilai jawaban : total nilai kuesioner)</i> | | | | | | | | |
| 01 | 3,671111111 | | | | | | 3,67 | |
| 02 | 3,6 | | | | | | 3,6 | |
| 03 | 3,644444444 | | | | | | 3,64 | |
| 04 | 3,551111111 | | | | | | 3,55 | |
| 05 | 3,386666667 | | | | | | 3,38 | |
| 06 | 3,222222222 | | | | | | 3,22 | |
| 06 | 3,475555556 | | | | | | 3,47 | |

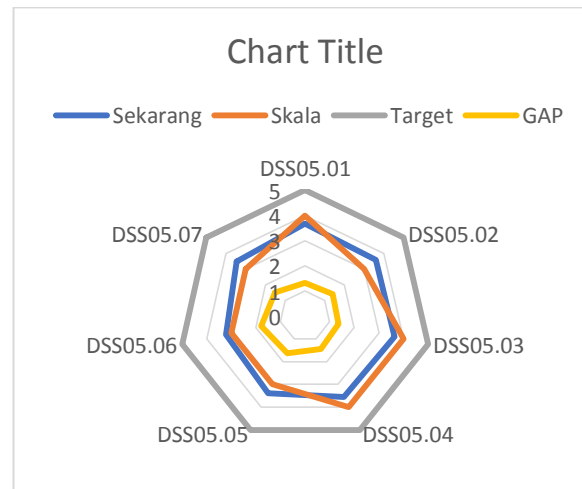
$$\text{Indeks kematangan} = \frac{\text{Jumlah nilai jawaban}}{\text{Total nilai Kuesioner}}$$

Dari perhitungan indeks kematangan terhadap data kuesioner didapatkan hasil seperti tabel di bawah ini :

Tabel 4.13 Hasil Indeks / Maturity Level

| DSS05 | Jumlah Jawaban | Jumlah Pertanyaan | <i>Indeks / Maturity Level saat ini</i> |
|-------|----------------|-------------------|---|
| 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 data tabel di atas akan dibandingkan antara *maturity level* saat ini dengan *maturity target* kemudian akan didapatkan *maturity GAP* seperti pada gambar di bawah ini :



Gambar 4.1 GAP Maturity Level

GAP maturity level di atas kemudian dapat dilakukan analisis sehingga ditetapkan *Maturity Level* setiap sub domain seperti pada tabel di bawah ini :

Tabel 4.14 Maturity Level sub domain DSS05

| Level | Sub Domain DSS05 | <i>Maturity Level</i> |
|-------|------------------|------------------------------|
| 4 | DSS05.01 | <i>Manage and Measurable</i> |
| 3 | DSS05.02 | <i>Defined Process</i> |
| 4 | DSS05.03 | <i>Manage and Measurable</i> |
| 4 | DSS05.04 | <i>Manage and Measurable</i> |
| 3 | DSS05.05 | <i>Defined Process</i> |
| 3 | DSS05.06 | <i>Defined Process</i> |
| 3 | DSS05.07 | <i>Defined Process</i> |

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

$$\begin{aligned}
 \text{Maturity level DSS05} &= \frac{\text{maturity level}}{\text{banyak proses}} \\
 &= \frac{(DSS05.01)+(DSS05.02)+(DSS05.03)+(DSS05.04)+DSS05.05+DSS05.06)+(DSS05.07)}{\text{Banyak Proses}}
 \end{aligned}$$

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

$$= 3,50$$

Jadi 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 organisasi.

4.2.3 Rekomendasi

Berdasarkan analisis Gap yang di dapat dari hasil level target yang ingin dicapai dan *level* yang tercapai pada DSS05, seperti pada Gambar 4.1 Rekomendasi yang dapat berikan untuk meningkatkan kualitas tingkat kematangan keamanan layanan jaringan di instansi tersebut:

- 1) Melindungi dari perangkat lunak berbahaya (DSS05.01) berada di dalam level 4 yaitu *Manage and measurable* pada instansi sudah melakukan prosedur dengan baik serta mampu melakukan pengembangan terkait perangkat lunak berbahaya.
- 2) Mengolah keamanan jaringan dan konektivitas (DSS05.02) berada di dalam level 3 yaitu *Defined process* pada instansi sudah mampu melakukan pengembangan terkait keamanan jaringan dan konektivitas. Menerapkan kebijakan terhadap ancaman-ancaman yang akan timbul bagi keamanan konektivitas .
- 3) Kelola keamanan titik akhir (DSS05.03) berada di dalam level 4 yaitu *Manage and measurable* pada instansi sudah mampu melakukan prosedur dengan sangat baik serta mampu melakukan pengembangan terkait sistem operasi perangkat dengan cara yang aman serta mengevaluasi keamanan layanan jaringan.
- 4) Kelola identitas pengguna dan akses logis (DSS05.04) berada di dalam level 4 yaitu *Manage and measurable* pada instansi sudah mampu melakukan prosedur

dengan sangat baik serta mampu melakukan penembangan terkait hak akses yang dimiliki setiap pengguna.

- 5) Mengelola akses fisik ke asset IT (DSS05.05) berada di dalam level 3 yaitu *Defined process* pada instansi sudah mampu melakukan pengembangan terkait akses keamanan fisik.
- 6) Kelola dokumen sensitif dan perangkat keluaran (DSS05.06) berada di dalam level 3 yaitu *Defined process* pada instansi sudah mampu melakukan pengembangan pengamanan fisik yang sesuai dengan target perlindungan.
- 7) Kelola kerentanan dan pantau infrastruktur untuk kejadian yang berhubungan dengan keamanan (DSS05.07) berada di dalam level 3 yaitu *Defined process* pada instansi sudah mampu melakukan pengembangan terkait keamanan yang telah dibuat saat pemantauan mengidentifikasi potensi kejadian keamanan.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah diperoleh maka dapat disimpulkan sebagai berikut :

- A. Kualitas keamanan layanan jaringan yang ada di Universitas Muhammadiyah Lamongan telah memenuhi standar keamanan yang diukur mengenai analisis DSS05 pada *framework* COBIT 2019 dengan parameter keamanan yaitu Kerahasiaan, intergritas dan ketersediaan. Keamanan sistem informasi pada level ini sudah baik, hanya masih membutuhkan inovasi dan pengembangan untuk siap, cepat dan tepat dalam penanganan ancaman keamanan. Instansi harus aktif membaca perkembangan teknologi keamanan dan segala bentuk ancamannya.
- B. Tingkat kematangan keamanan layanan jaringan menggunakan *framework* COBIT 2019 dengan *maturity level* di Universitas Muhammadiyah Lamongan sangat baik telah diukur berdasarkan sub domain DSS05 sub domain DSS05.01 dengan hasil indeks 3,67 menunjukkan pada level 4 yaitu *Manage and measurable*, DSS05.02 dengan hasil indeks 3,6 menunjukkan pada level 3 yaitu *Defined process*, DSS05.03 dengan hasil indeks 3,64 menunjukkan pada level 4 yaitu *Manage and measurable*, DSS05.04 dengan hasil indeks 3,55 menunjukkan pada level 4 yaitu *Manage and measurable*, DSS05.05 dengan hasil indeks 3,38 menunjukkan pada level 3 yaitu *Defined process*, DSS05.06 dengan hasil indeks 3,22 menunjukkan pada level 3 yaitu *Defined process*, dan DSS05.07 dengan hasil indeks 3,47 menunjukkan pada level 3 yaitu *Defined process*.

5.2 Saran

Adapun beberapa saran berikut ini dapat menjadi bahan masukan yang bermanfaat untuk pihak-pihak terkait antara lain :

- A. Bagi IT

Pihak IT untuk selalu menambah dan memaksimalkan pengembangan tingkat kematangan keamanan layanan jaringan dengan standar yang telah ditentukan.

B. Bagi Pembaca

Penelitian ini diharapkan dapat memberi manfaat untuk pembaca serta mendapatkan gambaran tentang analisis tingkat kematangan keamanan layanan jaringan menggunakan *framework* COBIT 2019 Dengan *Maturity Level*.

C. Bagi Peneliti Selanjutnya

Untuk peneliti selanjutnya diharapkan penelitian ini dapat dijadikan sebuah pijakan untuk melakukan penelitian yang lebih mendalam mengenai analisis tingkat kematangan keamanan layanan jaringan.

DAFTAR PUSTAKA

- Afifah, N., Firdaus, M. A., & Indah, D. R. (2018). *Evaluasi Tingkat Kematangan Menggunakan COBIT 5.0 DSS02 Pada Proses Pelayanan Indihome PT. Telekomunikasi Indonesia, tbk Sumatera Selatan (Doctoral dissertation, Sriwijaya University)*.
- Agoan, T. S., Wowor, H. F., & Karouw, S. (2017). Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan *Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)*. *Jurnal Teknik Informatika*, 10(1).
- Aleksi, A., & Afrina, M. (2022). *Pengukuran Tingkat Kematangan Layanan TI Pada UPT Perpustakaan Universitas Sriwijaya Menggunakan Framework COBIT 2019 (Doctoral dissertation, Sriwijaya University)*.
- Anastasia, P. N., & Atrinawati, L. H. (2020). Perancangan tata kelola teknologi informasi menggunakan *framework COBIT 2019* pada hotel xyz. *JSI: Jurnal Sistem Informasi (E-Journal)*, 12(2).
- Aprillya, M. R., Suryani, E., & Dzulkarnain, A. (2019). *System dynamics simulation model to increase paddy production for food security. Journal of Information Systems Engineering and Business Intelligence*, 5(1), 67-75.
- Aprillya, M. R., Suryani, E., & Dzulkarnain, A. (2019). *The analysis of quality of paddy harvest yield to support food security: A system thinking approach (case study: East Java)*. *Procedia Computer Science*, 161, 919-926.
- Ardiansyah, H., & Bianto, M. A. (2022). *Implementation of License Plate Recognition Monitoring System using Neural Network on Solar Powered Microcontroller. Indonesian Vocational Research Journal*, 2(1), 105-111.
- Bianto, M. A., Rahayu, S., Huda, M., & Kusriani, K. (2018). Perancangan Sistem Pendeteksi Plagiarisme Terhadap Topik Penelitian Menggunakan Metode *K-Means Clustering* dan Model Bayesian. *SEMNASTEKNOMEDIA ONLINE*, 6(1), 1-2.
- Cobit, F. T. M. F., & Santi, Z. S. Analisis Sistem Keamanan Jaringan Komputer Pada PT. Malindo.
- Fitriani, D. (2018). Analisis pengaruh penggunaan teknologi informasi terhadap kinerja karyawan PT. Asuransi Jiwasraya Pontianak. *Cogito Smart Journal*, 4(1), 160-170.

- Gusni, R. S. A., Kraugusteeliana, K., & Pradnyana, I. W. W. (2021). Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019. In *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya* (Vol. 2, No. 2, pp. 420-429).
- Handoyo, E. (2020). Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework COBIT 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800-55. *Jurnal CoSciTech (Computer Science and Information Technology)*, 1(2), 76-83.
- ISACA., 2011. *A Business Framework for the Governance and Management of Enterprise IT*.
- Jordy, W., Santoso, L. W., & Yulia, Y. (2022). Penerapan Manajemen Risiko IT pada Bank X dengan Menggunakan *Framework* COBIT 2019. *Jurnal Infra*, 10(1), 64-70.
- Kristanto, T., & Lestari, L. A. (2016). Analisis Tingkat Kematangan *E-Government* Menggunakan *Framework* COBIT 5 (Studi Kasus: Dinas Perdagangan dan Perindustrian Kota Surabaya). *Sesindo 2016, 2016*.
- Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA/ Jurnal Sistem Informasi Karya Anak Bangsa*, 2(01), 14-20.
- Nurchahyo, A. C., Pradana, M. G., & Hammad, R. (2020). Analisis Tingkat Kematangan Layanan Jaringan Berdasarkan Perspektif Internal Menggunakan COBIT 4.1 Pada Universitas Kristen Immanuel Yogyakarta. *Management and Sustainable Development Journal*, 2(1), 15-31.
- Prasetyo, A., Mariana, N., 2011. Analisis tata kelola teknologi informasi (IT governance) pada bidang akademik dengan COBIT framework studi kasus pada Universitas Stikubank Semarang. *Jurnal Teknologi Informasi DINAMIK*, 16(2), 139-149.
- Prasetyo, T. M. A., & Sitokdana, M. N. (2021). Analisis Tata Kelola Pusat Data dan Informasi Kementerian xyz Menggunakan COBIT 2019. *Journal of Applied Computer Science and Technology*, 2(2), 95-107.
- Putra, S. D., Herman, H., & Yudhana, A. (2022). Evaluasi Tata Kelola Layanan Jaringan Menggunakan COBIT 2019 Pada Sekolah Tinggi Ilmu Kesehatan. *Resistor (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer)*, 5(2), 119-126.

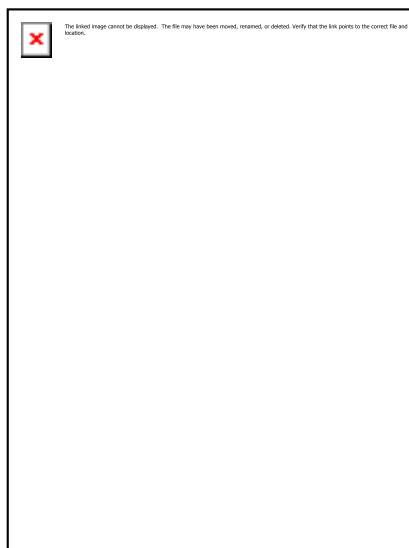
- Rahim, F. R., Suherman, D. S., & Murtiani, M. (2019). Analisis Kompetensi Guru dalam Mempersiapkan Media Pembelajaran Berbasis Teknologi Informasi Era Revolusi Industri 4.0. *Jurnal Eksakta Pendidikan (Jep)*, 3(2), 133-141.
- Rahmawati, D. (2008). Analisis Faktor Faktor yang Berpengaruh Terhadap Pemanfaatan Teknologi Informasi. *Jurnal Ekonomi dan Pendidikan*, 5(1).
- Rosmiati, Riadi, I., Prayudi, Y., 2016. *A Maturity level framework for measurement of information security performance. International Journal of Computer Applications*, 141(8), 975–8887
- Saleh, M., Yusuf, I., & Sujaini, H. (2021). Penerapan *Framework* COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas. *Jepin (Jurnal Edukasi dan Penelitian Informatika)*, 7(2), 204-209.
- Setiawan, R. A., & Wasilah, W. (2022, August). Evaluasi Tata Kelola Dan Manajemen Teknologi Informasi Menggunakan *Framework* COBIT 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung Selatan. In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, pp. 8-15).
- Shodiq, M., & Saputra, B. D. (2022). *Grey Forecasting* Model Untuk Peramalan Harga Ikan Budidaya. *JURIKOM (Jurnal Riset Komputer)*, 9(6), 1770-1778.
- Surendro, K. (2009) Implementasi Tata Kelola Teknologi Informasi Bandung: Informatika
- Syaputra, S. D. Jurnal Tata Kelola Teknologi Informasi Menggunakan *Framework* COBIT 5 PT Santani Agro Persada.
- Team, C. P. (2010). *CMMI for Services*, Version 1.3. *CMU SEI*, Nov-2010.
- Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan *Framework* COBIT 5 Menggunakan *Capability Maturity Model Integration* (CMMI). *J. Sist. Inf. Bisnis*, 9(1), 47.
- Umar, R., Riadi, I., Handoyo, E., (2017). Analisis Tata kelola teknologi informasi menggunakan *framework* COBIT 5 Pada Domain *Delivery, Service, And Support* (DSS). In *Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017* (pp. 41–48).
- Umar, R., Riadi, I., Zamroni, G. M., 2018. *Mobile Forensic tools evaluation for digital crime investigation. International Journal on Advanced Science, Engineering and Information Technology (IJASEIT)*, 8(3), 949.

- Wulung, G. L., Rindengan, Y., & Sentinuwo, S. R. (2021). Implementasi COBIT 5 *Deliver, Service, and Support* Untuk Mengukur Kematangan Dinas Komunikasi Dan Informatika Kota Manado.
- Yunus, I. R., Agitha, N., & Anjarwani, S. E. A. (2019). Analisis Tata Kelola Teknologi Informasi pada Layanan Infrastruktur Jaringan RSUD Provinsi NTB menggunakan COBIT 4.1. *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*, 1(1), 19-30.
- Yusuf, Y., Gunawan, E. T., & Sarita, R. (2021). Analisis Tingkat Kematangan Pelayanan Pada PT Telkom Sampit dengan Menggunakan Domain COBIT 5 DSS02 dan DSS03. *Journal of Information System Research (JOSH)*, 2(4), 283-287.

LAMPIRAN

Lampiran 1 penyebaran kuesioner kepada responden

1. Responden pihak IT Universitas Muhammadiyah Lamongan



2. Responden Dosen Universitas Muhammadiyah Lamongan



3. Responden Mahasiswa Universitas Muhammadiyah Lamongan

