

# EVALUASI TINGKAT KAPABILITAS E-GOVERNMENT DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN LAMONGAN MENGGUNAKAN FRAMEWORK COBIT 5

Mohammad Farizd<sup>1\*</sup>, Siti Mukaromah<sup>2</sup>, Anita Wulansari<sup>3</sup>

<sup>1,2,3</sup>Universitas Pembangunan Nasional “Veteran” Jawa Timur; Jl. Rungkut Madya No.1, Gunung Anyar, Surabaya, Jawa Timur; (031) 8706369

Received: 5 Juli 2024

Accepted: 31 Juli 2024

Published: 7 Agustus 2024

## Keywords:

Kapabilitas; e-Government; Keamanan; Risiko; COBIT 5.

## Correspondent Email:

mohammadfarizd4@gmail.com

**Abstrak.** Penerapan teknologi informasi berperan penting dalam menyediakan dan menyederhanakan proses bisnis terhadap sebuah instansi. Dinas Komunikasi dan Informatika Kabupaten Lamongan telah melakukan pengimplementasian e-government atau sering dikenal dengan SPBE. Dalam pelaksanaan manajemen risiko keamanan informasi pada e-government di Diskominfo Kabupaten Lamongan masih belum mencapai tingkat optimal. Sehingga perlu diperlukannya pengukuran tingkat kapabilitas melalui penerapan kerangka kerja COBIT 5 dengan proses yang diukur yaitu APO12 Mengelola Risiko, APO13 Mengelola Keamanan, dan DSS05 Mengelola Layanan Keamanan. Hasil tingkat kapabilitas dari manajemen risiko keamanan informasi pada Diskominfo Kabupaten Lamongan terhadap proses APO12 dan DSS05 berada level 1 sedangkan APO13 mencapai pada level 2. Dengan demikian, ketiga proses tersebut telah dijalankan dan sebagian besar pencapaiannya didukung oleh bukti yang cukup serta untuk proses APO13 telah diterapkan dan dikelola dengan tepat.

**Abstract.** The application of information technology plays an important role in providing and simplifying business processes for an agency. The Communication and Information Technology Office of Lamongan Regency has implemented e-government or often known as SPBE. In the implementation of information security risk management in e-government at Diskominfo Lamongan Regency, it still has not reached the optimal level. So it is necessary to measure the level of capability through the application of the COBIT 5 framework with the measured processes, namely APO12 Managing Risk, APO13 Managing Security, and DSS05 Managing Security Services. The results of the capability level of information security risk management at the Lamongan Regency Diskominfo for the APO12 and DSS05 processes are level 1 while APO13 reaches level 2. Thus, the three processes have been carried out and most of their achievements are supported by sufficient evidence and for the APO13 process has been implemented and managed appropriately.

## 1. PENDAHULUAN

Peran teknologi informasi sangat signifikan dalam membantu dan menyederhanakan proses bisnis di dalam sebuah organisasi. Penggunaan teknologi informasi di sektor pemerintahan sangat penting untuk menciptakan proses pemerintahan yang optimal dengan mengimplementasikan prinsip tata kelola yang

baik (*good governance*) [1]. Penerapan teknologi informasi dalam lembaga pemerintahan biasa dikenal dengan konsep *e-government*, dimana di Indonesia biasa dikenal dengan Sistem Pemerintahan Berbasis Elektronik (SPBE).

Adanya e-government (SPBE) merupakan upaya pemerintah untuk memanfaatkan

teknologi informasi untuk pengimplementasian sistem pemerintahan dengan baik, sehingga dapat mengurangi beberapa kesalahan yang disebabkan human error [2]. Seiring perkembangan teknologi, data dan informasi banyak kali disalahgunakan oleh individu yang tidak bertanggung jawab, sehingga semua institusi publik bertanggung jawab atas bahaya dan gangguan keamanan siber. Selain itu diharapkan upaya tidak terjadinya IT Productivity Paradox pada instansi pemerintahan, dikarenakan TI yang diimplementasikan tidak sesuai dengan proses bisnis yang berjalan [3]. Maka dari itu, keamanan data informasi yang optimal hanya dapat dicapai melalui implementasi berbagai usaha teknis yang didukung oleh prosedur dan kebijakan manajemen yang tepat [4].

Dinas Komunikasi dan Informatika Kabupaten Lamongan yaitu sebuah organisasi perangkat daerah (OPD) di mana bertanggung jawab terhadap bidang komunikasi dan informatika, serta urusan pemerintahan terkait persandian dan statistik. Penerapan e-government di Kabupaten Lamongan didukung dengan adanya Sistem Pemerintahan Berbasis Elektronik yang telah berkembang signifikan. Namun, dalam pelaksanaan manajemen risiko keamanan informasi terhadap SPBE di Dinas Komunikasi dan Informatika Kabupaten Lamongan masih belum mencapai tingkat optimal saat ini. Maka dari itu, untuk mengimplementasikan TI secara optimal, diperlukan standar tata kelola TI.

Standar ini berupa aturan yang memastikan tujuan TI selaras dengan tujuan bisnis perusahaan, seperti COBIT, ITIL, ISO/IEC 270001, dan lain sebagainya. Masing-masing standar tata kelola ini digunakan untuk mengelola kondisi tertentu. Kerangka kerja ITIL digunakan sebagai kumpulan praktik untuk aktivitas TI, seperti manajemen layanan TI dan manajemen aset TI, yang berfokus pada bagaimana layanan TI dapat disesuaikan dengan kebutuhan bisnis [5], [6]. ISO/IEC 27001 digunakan sebagai standar untuk sistem manajemen keamanan informasi [5], [7]. COBIT saat ini masih terus berkembang dari satu versi hingga versi terbarunya yakni COBIT 2019 [8]. Namun, banyak penelitian masih memanfaatkan versi COBIT 4.1 dan COBIT 5.0, bukan versi terbaru COBIT 2019 [9]. Sehingga untuk mengevaluasi sejauh mana

pengelolaan manajemen risiko keamanan informasi tersebut, perlu dilakukan pengukuran tingkat kapabilitas dengan memanfaatkan framework COBIT 5.

COBIT 5 telah banyak diterapkan di perusahaan, membuatnya lebih mudah bagi perusahaan untuk menerapkannya serta dapat memberikan pendekatan komprehensif dan praktis tentang bagaimana proses bisnis dan TI berhubungan satu sama lain [10], [11]. Penggunaan proses COBIT 5 untuk keamanan perusahaan yang paling penting berfokus pada tiga proses yaitu APO12, APO13, dan DSS05 [12]. Ketiga proses tersebut memiliki tujuan untuk memastikan bahwa kejadian dan dampak dari peristiwa keamanan informasi tidak melampaui tahap risiko yang telah ditetapkan dari perusahaan [13].

Penelitian ini berfokus pada tiga proses yaitu APO12 Mengelola Risiko, APO13 Mengelola Keamanan, dan DSS05 Mengelola Layanan Keamanan yang akan dipakai untuk mengevaluasi e-government Dinas Komunikasi dan Informatika Kabupaten Lamongan. Dengan demikian penelitian ini memiliki tujuan untuk memberikan penilaian terhadap tingkat kapabilitas e-government di Dinas Komunikasi dan Informatika Kabupaten Lamongan beserta saran untuk perbaikan untuk kedepannya.

## 2. TINJAUAN PUSTAKA

### 2.1. Audit Sistem Informasi

Proses pengumpulan dan evaluasi bukti untuk menilai kemampuan sistem informasi untuk menjaga aset, kerahasiaan data, membantu pemenuhan tujuan organisasi, dan menggunakan sumber daya secara efisien dikenal dikenal audit sistem informasi [14].

### 2.2. Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi (IT Governance) umumnya merujuk pada kumpulan prosedur, kebijakan, dan tindakan yang diterapkan oleh organisasi untuk memastikan bahwa struktur dan proses teknologi informasi mendukung dan selaras dengan tujuan organisasi [15]. Tujuannya Memastikan penggunaan teknologi informasi yang efisien dan efektif untuk mencapai tujuan perusahaan, meningkatkan kualitas layanan, mengurangi risiko, dan memastikan kepatuhan terhadap peraturan dan kebijakan yang berlaku

adalah tujuan utama tata kelola teknologi informasi [16].

**2.3. Keamanan Informasi**

Keamanan Informasi merupakan langkah-langkah demi menjaga keamanan aset data dari berbagai potensi bahaya. Secara umum, perlindungan data memastikan kelangsungan bisnis, meminimalisir risiko, serta meningkatkan pengembalian investasi [17].

**2.4. Control Objective for Information and Related Technology 5 (COBIT 5)**

COBIT 5 pertama kali dirilis pada 2012, dimana merupakan panduan standar yang membantu perusahaan menghasilkan nilai, menyelaraskan organisasi, serta mencapai tujuan dari pengelolaan manajemen teknologi informasi dan tata kelola yang optimal [18]. COBIT 5 mencakup berbagai jenis perusahaan, termasuk yang berorientasi komersial, nirlaba, serta sektor publik seperti organisasi, pemerintahan, perusahaan, atau entitas lainnya, dan memberikan manfaat yang luas bagi mereka [19], [20]. Selain itu, COBIT 5 merupakan sebuah framework yang keseluruhan yang membantu perusahaan mencapai tujuan mereka terkait manajemen TI dan tata kelola perusahaan [19]. Dalam COBIT 5 mempunyai panduan proses penilaian yang mana menyediakan berbagai tahapan untuk melakukan penilaian yaitu menggunakan panduan Process Assessment Model (PAM) COBIT 5 dan Self-Assessment Guide Using COBIT 5 [21], [22].

**2.5. RACI Chart**

Diagram RACI berasal dari kata Responsible, Accountable, Consulted, dan Informed merupakan matriks yang menggambarkan tindakan dan wewenang organisasi atau perusahaan terhadap proses pengambilan Keputusan [11].

**2.6. Dimensi Kapabilitas**

Dalam dokumen panduan Process Assessment Model COBIT 5, dimensi kapabilitas telah dijelaskan dengan memanfaatkan model penilaian standar dari ISO/IEC 15504 untuk mengevaluasi kapabilitas di setiap domain proses [21]. Berikut tabel 1 merupakan tingkatan level untuk penilaian proses dan kapabilitas COBIT 5.

LEVEL	KETERANGAN
0	Proses Tidak Lengkap
1	Proses yang Dilakukan
2	Proses yang Dikelola
3	Proses yang telah ditetapkan
4	Proses yang Dapat Diprediksi
5	Mengoptimalkan Proses

Tabel 1. Tingkatan Kapabilitas

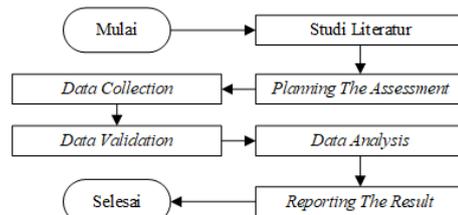
**2.7. Skala Penilaian**

Berikut tabel 2 merupakan skala penilaian yang menggunakan metode evaluasi yang telah didefinisikan COBIT 5 berdasarkan standar ISO/IEC 15504 [21].

SKALA	KETERANGAN
<i>Not Achieved</i> (N) 0 hingga 15%	Skala kategori N menunjukkan sedikit atau tidak ada bukti pencapaian dari atribut proses yang dinilai.
<i>Partially Achieved</i> (P) 15% hingga 50%	Skala kategori P, terdapat beberapa bukti yang mendekati beberapa pencapaian dari atribut yang dinilai.
<i>Largely Achieved</i> (L) 50% hingga 85%	Skala kategori L, terdapat bukti pendekatan sistematis terhadap pencapaian yang signifikan dari atribut proses yang dinilai.
<i>Fully Achieved</i> (F) 85% hingga 100%	Skala kategori F, terdapat bukti pendekatan yang lengkap dan sistematis dengan pencapaian penuh dari atribut yang dinilai.

Tabel 2. Skala NPLF

**3. METODE PENELITIAN**



Gambar 1. Alur Penelitian

**3.1. Studi Literatur**

Pada tahap ini digunakan untuk pencarian literatur yang relevan dengan objek penelitian untuk mendukung pelaksanaan penelitian.

**3.2. Planning The Assessment**

Tujuan dari tahap kedua adalah untuk menganalisis RACI Chart sebagai dasar untuk memahami citra organisasi dan mengidentifikasi responden wawancara berdasarkan dari struktur organisasi.

**3.3. Data Collection**

Tujuan pengumpulan data adalah untuk memperoleh data penelitian melalui observasi dan wawancara.

### 3.4. Data Validation

Validasi data adalah untuk memvalidasi temuan yang dihasilkan selama proses pengumpulan data.

### 3.5. Data Analysis

Analisis data adalah untuk memberi level pada setiap proses dan menentukan tingkat kapabilitas berdasarkan tingkat observasi yang dilakukan.

### 3.6. Reporting The Result

Tahapan reporting the result yang berisikan tentang hasil pengukuran kapabilitas dan saran rekomendasi untuk perbaikan.

## 4. HASIL DAN PEMBAHASAN

### 4.1. Planning The Assessment

Penentuan responden berfokus pada indikator yang berkategori Responsible "R", pada kategori tersebut memiliki tanggung jawab langsung dalam pelaksanaan kegiatan. Berikut tabel 3 mengenai pemetaan responden dari RACI Chart COBIT 5 dengan struktur fungsional di Dinas Komunikasi dan Informatika Kabupaten Lamongan.

RA CI	Peran	Struktur Fungsional Organisasi	Proses
R	Business Process Owners	Kepala Seksi Tata Kelola dan Pemberdayaan TIK	APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06
R	Information Security Manager	Kepala Seksi Persandian dan Keamanan Informasi	APO13.01, APO13.02, APO13.03
R	Head Development	Kepala Seksi Pengembangan Aplikasi dan Integrasi Sistem Informasi	DSS05.01, DSS05.02, DSS05.03
R	Head IT Operations	Kepala Seksi Pengembangan Infrastruktur TIK	DSS05.04, DSS05.05, DSS05.06, DSS05.07

Tabel 3. Pemetaan Narasumber

### 4.2. Data Analysis

Berikut merupakan penilaian dan pemberian level pada setiap proses, serta menentukan tingkat kapabilitas berdasarkan observasi data

yang telah diperoleh dan diverifikasi sebelumnya.

#### 4.2.1. APO12 – Mengelola Risiko

Berikut tabel 4 dan 5 menunjukkan hasil penilaian praktik dasar proses dan produk kerja APO12 Mengelola Risiko.

Tujuan Proses	Praktik Dasar	Nilai Praktik Dasar	Nilai Tujuan Proses
APO12-O1 Risiko terkait TI diidentifikasi, dianalisis, dikelola, dan dilaporkan.	APO12-BP1 Mengumpulkan data	47.14%	44.99%
	APO12-BP2 Menganalisis risiko	42.85%	
APO12-O2 Tersedia profil risiko terkini dan lengkap.	APO12-BP3 Memelihara profil risiko	28.57%	28.57%
APO12-O3 Semua tindakan manajemen risiko yang signifikan dikelola dan terkendali.	APO12-BP4 Mengartikulasikan risiko	40%	32.91%
	APO12-BP5 Menentukan portofolio tindakan manajemen risiko	15%	
	APO12-BP6 Menanggapi risiko	43.75%	
APO12-O4 Tindakan-tindakan manajemen risiko dilaksanakan secara efektif	APO12-BP2 Menganalisis risiko	42.85%	32.61%
	APO12-BP4 Mengartikulasikan risiko	40%	
	APO12-BP5 Menentukan portofolio tindakan manajemen risiko	15%	

Tabel 4. Hasil Penilaian Praktik Dasar APO12

Berdasarkan tabel 4, persentase rata rata tujuan proses APO12 sebesar 34.77% berada skala P (Partially Achieved). Dimana proses pengelolaan risiko di Dinas Komunikasi dan Informatika Kabupaten Lamongan terdapat beberapa aspek belum memenuhi kriteria kinerja praktik yang diharapkan. Beberapa praktik, seperti pencatatan, pengelolaan, dan identifikasi peristiwa risiko, masih belum dilakukan secara optimal.

Produk Kerja	Ada/Tidak	Nilai
APO12-WP1 Data tentang situasi lingkungan operasi yang berkaitan dengan risiko	Y	100%
APO12-WP2 Data tentang risiko kejadian dan faktor penyebabnya	Y	
APO12-WP3 Masalah dan faktor risiko yang muncul	Y	
APO12-WP4 Ruang lingkup upaya analisis risiko	Y	100%
APO12-WP5 Skenario dari risiko TI	Y	
APO12-WP6 Hasil analisis risiko	Y	100%
APO12-WP7 Skenario risiko yang terdokumentasi berdasarkan lini bisnis dan fungsi	Y	
APO12-WP8 Profil risiko agregat, termasuk status tindakan manajemen risiko	Y	66.66%
APO12-WP9 Analisis risiko dan laporan profil risiko untuk para pemangku kepentingan	Y	
APO12-WP10 Meninjau hasil penilaian risiko dari pihak ketiga	Y	0%
APO12-WP11 Peluang untuk menerima risiko yang lebih besar	T	
APO12-WP12 Proposal proyek untuk mengurangi risiko	T	100%
APO12-WP13 Rencana tanggap darurat terkait risiko	Y	
APO12-WP14 Komunikasi dampak risiko	Y	100%
APO12-WP15 Akar permasalahan terkait risiko	Y	

Tabel 5. Hasil Penilaian Produk Kerja APO12

Berdasarkan tabel 5, persentase rata rata produk kerja APO12 sebesar 77.77% berada skala L (Largely Achieved). Adanya produk kerja merupakan sebagai pembuktian dimana praktik dasar telah dilaksanakan. Setelah itu, produk kerja dan skor rata-rata praktik dasar dihitung untuk menghasilkan skor keseluruhan proses pada APO12 [23], seperti pada gambar 2.

Nilai Outcomes	$\frac{(44.99 + 28.57 + 32.91 + 32.61)}{4} \%$	34.77% (P)
Nilai Work Product	$\frac{(100 + 100 + 100 + 66.66 + 0 + 100)}{6} \%$	77.77% (L)
Nilai Proses	$\frac{(34.77 + 77.77)}{2} \%$	56.27% (L)

Gambar 2. Perhitungan Persentase Tujuan Proses dan Produk Kerja APO12

Berdasarkan perhitungan, proses APO12 memperoleh persentase 56.27% dengan skala L (Largely Achieved). Karena tidak memenuhi kategori F (Fully Achieved), APO12 ada di level 1 dan tidak dapat naik ke level 2 [13].

#### 4.2.2. APO13 – Mengelola Keamanan

Berikut tabel 6, 7, 8 dan 9 menunjukkan hasil penilaian praktik dasar proses dan produk kerja APO13 Mengelola Keamanan.

Tujuan Proses	Praktik Dasar	Nilai Praktik Dasar	Nilai Tujuan Proses
APO13-O1 Tersedia sistem yang mempertimbangkan dan secara efektif menangani persyaratan keamanan informasi perusahaan.	APO13-BP1 Menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (SMKI)	100%	92.5%
	APO13-BP3 Memantau dan meninjau Sistem Manajemen Keamanan Informasi (SMKI)	85%	
APO13-O2 Rencana keamanan telah dibuat, diterima dan dikomunikasikan di seluruh perusahaan.	APO13-BP2 Mendefinisikan rencana perawatan dan mengelola risiko keamanan informasi	85.71%	85.71%
APO13-O3 Penerapan keamanan informasi diterapkan dan dioperasikan secara konsisten di seluruh perusahaan.	APO13-BP3 Memantau dan meninjau Sistem Manajemen Keamanan Informasi (SMKI)	85%	85%

Tabel 6. Hasil Penilaian Praktik Dasar APO13

Berdasarkan tabel 6 persentase rata rata tujuan proses APO13 sebesar 87.73% berada skala F (Fully Achieved). Proses pengelolaan keamanan di Dinas Komunikasi dan Informatika Kabupaten Lamongan sudah cukup baik, namun beberapa aspek masih kurang optimal, seperti peninjauan, pemantauan, dan pendokumentasian terkait aktivitas pengelolaan keamanan.

Produk Kerja	Ada/Tidak	Nilai
APO13-WP1 Kebijakan SMKI	Y	100%
APO13-WP2 Pernyataan cakupan SMKI	Y	
APO13-WP3 Rencana penanganan risiko keamanan informasi	Y	100%
APO13-WP4 Studi Kasus bisnis keamanan informasi	Y	

<b>APO13-WP5</b> Laporan audit SMKI	Y	100%
<b>APO13-WP6</b> Rekomendasi untuk meningkatkan SMKI	Y	

Tabel 7. Hasil Penilaian Produk Kerja APO13

Berdasarkan tabel 7 persentase rata rata produk kerja APO13 sebesar 100% berada skala F (Fully Achieved). Adanya produk kerja merupakan sebagai pembuktian dimana praktik dasar telah diterapkan. Selanjutnya, nilai dasar praktik dan produk kerja rata-rata dihitung untuk menentukan nilai keseluruhan proses APO13, seperti pada gambar 3.

Nilai Outcomes	$\frac{(92.5 + 85.71 + 85)}{3}$ %	87.73% (F)
Nilai Work Product	$\frac{(100 + 100 + 100)}{3}$ %	100% (F)
Nilai Proses	$\frac{(87.73 + 100)}{2}$ %	93.86% (F)

Gambar 3. Perhitungan Persentase Tujuan Proses dan Produk Kerja APO13

Berdasarkan perhitungan, proses APO13 memperoleh persentase 93.86% dengan skala F (Fully Achieved). Sehingga proses APO13 dapat dilanjutkan ke tingkat kapabilitas berikutnya karena telah memenuhi kriteria rating F (Fully Achieved). Dengan demikian, penilaian akan diteruskan ke level 2 (managed process), yang mencakup indikator PA 2.1 Performance Management dan PA 2.2 Work Product Management.

Generic Practices (GPs)	Ada/Tidak	Generic Work Products (GWPs)	Ada/Tidak
<b>GP 2.1.1</b> Mengidentifikasi tujuan-tujuan untuk kinerja proses terkait pengelolaan keamanan.	Y	<b>GWP 1.0</b> Dokumentasi proses terkait ruang lingkup proses.	Y
		<b>GWP 2.0</b> Rencana proses harus memberikan rincian tujuan kinerja proses.	Y
<b>GP 2.1.2</b> Merencanakan dan memantau kinerja proses untuk memenuhi tujuan yang telah diidentifikasi mengenai mengelola keamanan.	Y	<b>GWP 2.0</b> Rencana proses harus memberikan rincian tujuan kinerja proses.	Y
		<b>GWP 9.0</b> Catatan kinerja proses harus memberikan rincian hasil.	T

<b>GP 2.1.3</b> Menyesuaikan kinerja proses dalam pengelolaan keamanan.	T	<b>GWP 4.0</b> Catatan kualitas harus memberikan rincian tindakan yang diambil ketika kinerja tidak tercapai.	T
<b>GP 2.1.4</b> Menetapkan tanggung jawab dan wewenang untuk melaksanakan proses dalam mengelola keamanan.	Y	<b>GWP 1.0</b> Dokumentasi proses harus memberikan rincian pemilik proses dan siapa yang bertanggung jawab.	Y
		<b>GWP 2.0</b> Rencana proses harus mencakup rincian rencana komunikasi proses.	Y
<b>GP 2.1.5</b> Mengidentifikasi dan menyediakan sumber daya untuk melaksanakan proses sesuai rencana pengelolaan Keamanan.	T	<b>GWP 2.0</b> Rencana proses harus memberikan rincian rencana pelatihan proses dan rencana sumber daya proses.	T
<b>GP 2.1.6</b> Mengelola antarmuka antara pihak-pihak yang terlibat.	Y	<b>GWP 1.0</b> Dokumentasi proses harus memberikan rincian individu dan kelompok yang terlibat (pemasok, pelanggan, dan RACT).	Y
		<b>GWP 2.0</b> Rencana proses harus memberikan rincian rencana komunikasi proses.	Y
<b>Nilai Rata-Rata</b>	66.66 %	<b>Nilai Rata-Rata</b>	70%

Tabel 8. Hasil Penilaian PA 2.1 Peromance Management APO13

Berdasarkan tabel 8, hasil penilaian PA 2.1 Performance Management menunjukkan nilai persentase GPs sebesar 66,66% dan GWPs sebesar 70%. Rata-rata persentase performance management adalah 68,33%, yang masuk kedalam kategori L (Largely Achieved).

Generic Practices (GPs)	Ada/Tidak	Generic Work Products (GWPs)	Ada/Tidak
GP 2.2.1 Mendefinisikan persyaratan untuk produk kerja, termasuk struktur konten dan kriteria kualitas.	Y	GWP 3.0 Rencana kualitas harus memberikan rincian kriteria kualitas dan konten serta struktur produk kerja.	Y
GP 2.2.2 Menentukan persyaratan untuk dokumentasi dan kontrol produk kerja.	Y	GWP 1.0 Dokumentasi proses harus memberikan rincian kontrol (matriks kontrol).	Y
		GWP 3.0 Rencana kualitas harus memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi dan kontrol perubahan.	T
GP 2.2.3 Mengidentifikasi, mendokumentasikan, dan mengendalikan produk kerja.	T	GWP 3.0 Rencana kualitas harus memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi, dan pengendalian perubahan.	T
GP 2.2.4 Meninjau dan menyesuaikan produk kerja untuk memenuhi persyaratan yang ditetapkan.	Y	GWP 4.0 Terdapat menyediakan jejak audit dari tinjauan yang dilakukan.	Y
<b>Nilai Rata-Rata</b>	75%	<b>Nilai Rata-Rata</b>	60%

Tabel 9. Hasil Penilaian PA 2.2 Work Product Management APO13

Berdasarkan tabel 9, penilaian PA 2.2 Work Product Management menunjukkan presentase GPs sebesar 75% dan GWPs sebesar 60%. Sehingga rata-rata persentase manajemen produk kerja adalah 67,5%, termasuk dalam kategori L (Largely Achieved).

PA 2.1 Performance Management	Nilai Generic Practices	$\frac{4}{6}$ %	66.66% (L)
	Nilai Generic Work Products	$\frac{7}{10}$ %	70% (L)
	Nilai Level 2 PA 2.1	$\frac{(66.66 + 70)}{2}$ %	68.33% (L)
PA 2.2 Work Product Management	Nilai Generic Practices	$\frac{3}{4}$ %	75% (L)
	Nilai Generic Work Products	$\frac{3}{5}$ %	60% (L)
	Nilai Level 2 PA 2.2	$\frac{(100 + 80)}{2}$ %	67.5% (L)

Gambar 4. Perhitungan Persentase PA 2.1 dan PA 2.2 APO13

Berdasarkan hasil perhitungan akhir gambar 4, nilai persentase untuk performance management dalam proses APO13 adalah 68,33%, masuk dalam kategori L (Largely Achieved). Sementara itu, nilai untuk work product management adalah 67,5%, masuk pada kategori L (Largely Achieved). Maka dari itu, tingkat kapabilitas proses domain APO13 hanya mencapai level 2, karena kriteria F (Fully Achieved) tidak terpenuhi.

#### 4.2.3. DSS05 – Mengelola Layanan Keamanan

Berikut adalah tabel 10 dan 11 menunjukkan hasil penilaian praktik dasar proses dan produk kerja DSS05 Mengelola Layanan Keamanan.

Tujuan Proses	Praktik Dasar	Nilai Praktik Dasar	Nilai Tujuan Proses
DSS05-O1 Penerapan keamanan jaringan dan komunikasi memenuhi kebutuhan bisnis.	DSS05-BP1 Melindungi dari malware	100%	75%
	DSS05-BP2 Mengelola konektivitas keamanan jaringan	100%	
	DSS05-BP7 Memantau peristiwa kejadian infrastruktur keamanan	25%	
DSS05-O2 Informasi yang diproses, disimpan, dan dikirimkan oleh perangkat titik akhir.	DSS05-BP1 Melindungi dari malware	100%	87.5%
	DSS05-BP3 Mengelola keamanan pada endpoint	75%	
DSS05-O3 Setiap pengguna diidentifikasi secara unik dan memiliki hak akses sesuai dengan peran bisnis mereka.	DSS05-BP4 Mengelola identitas pengguna dan logika akses	84.37%	84.37%

<b>DSS05-O4</b> Perlindungan fisik telah diterapkan untuk melindungi informasi dari akses yang tidak sah, kerusakan, dan gangguan saat diproses, disimpan, atau ditransmisikan.	<b>DSS05-BP5</b> Mengelola akses fisik ke aset TI	75%	75%
<b>DSS05-O5</b> Informasi elektronik diamankan dengan baik saat disimpan, dikirim, atau dimusnahkan.	<b>DSS05-BP6</b> Mengelola dokumen sensitif dan perangkat output	60%	60%

Tabel 10. Hasil Penilaian Praktik Dasar DSS05

Berdasarkan tabel 10, persentase rata rata tujuan proses DSS05 sebesar 76.37% berada skala L (Largely Achieved). Proses manajemen layanan keamanan di Dinas Komunikasi dan Informatika Kabupaten Lamongan terdapat beberapa aspek belum memenuhi kriteria kinerja praktik. Beberapa praktik seperti pemantauan, pengelolaan, dan pendokumentasian aktivitas layanan keamanan belum dilaksanakan secara optimal.

Produk Kerja	Ada/Tidak	Nilai
<b>DSS05-WP1</b> Kebijakan pencegahan perangkat lunak berbahaya	Y	100%
<b>DSS05-WP2</b> Evaluasi potensi ancaman	Y	
<b>DSS05-WP3</b> Kebijakan keamanan konektivitas	Y	100%
<b>DSS05-WP4</b> Hasil uji penetrasi	Y	
<b>DSS05-WP5</b> Kebijakan keamanan untuk perangkat endpoint	Y	100%
<b>DSS05-WP6</b> Hak akses pengguna yang disetujui	T	
<b>DSS05-WP7</b> Hasil tinjauan terhadap akun dan hak istimewa pengguna	T	0%
<b>DSS05-WP8</b> Permintaan akses yang disetujui	Y	
<b>DSS05-WP9</b> Akses log	T	50%
<b>DSS05-WP10</b> Inventarisasi dokumen dan perangkat sensitif	Y	
<b>DSS05-WP11</b> Hak akses istimewa	T	33.33%
<b>DSS05-WP12</b> Log peristiwa keamanan	T	
<b>DSS05-WP13</b> Karakteristik insiden keamanan	Y	
<b>DSS05-WP14</b> Tiket insiden keamanan	T	

Tabel 11. Hasil Penilaian Produk Kerja DSS05

Berdasarkan tabel 11 persentase rata rata produk kerja DSS05 sebesar 61.9% berada skala L (Largely Achieved). Adanya produk kerja merupakan sebagai pembuktian dimana praktik dasar telah diterapkan. Setelah itu, nilai rata-rata dasar praktik dan produk kerja dihitung untuk menentukan nilai keseluruhan domain DSS05, seperti pada gambar 5.

Nilai Outcomes	$\frac{(75 + 87.5 + 84.37 + 75 + 60)}{5}$ %	76.37% (L)
Nilai Work Product	$\frac{(100 + 100 + 100 + 0 + 50 + 50 + 33.33)}{7}$ %	61.9% (L)
Nilai Proses	$\frac{(76.37 + 61.9)}{2}$ %	69.13% (L)

Gambar 5. Perhitungan Persentase Tujuan Proses dan Produk Kerja DSS05

Berdasarkan hasil perhitungan gambar 5, proses DSS05 memperoleh persentase 69.13% dengan skala L (Largely Achieved). Oleh karena itu, DSS05 berada pada tingkatan level 1 dan tidak dapat dilanjutkan ke level 2 karena tidak memenuhi kategori F (Fully Achieved).

### 4.3. Reporting The Result

COBIT 5 Proses	Level 0	Level 1		Level 2	
		PA 1.1	PA 2.1	PA 2.2	
APO12	F 100%	L 56.27%			
APO13	F 100%	F 93.86%	L 68.33%	L 67.5%	
DSS05	F 100%	L 69.13%			

Tabel 12. Hasil Penilaian Tingkat Kapabilitas

Berdasarkan hasil pengukuran pada tabel 12, tingkat kapabilitas proses APO12 dan DSS05 berada pada tingkat kapabilitas level 1 (performed process), dengan nilai persentase 56,27% dan 69,13%, berkategori L (largely achieved). Dimana sebagian besar prosedur APO12 dan DSS05 pada level 1 telah dilaksanakan dan didukung oleh bukti yang kuat. Sementara itu, untuk proses domain APO13 mencapai tingkat kemampuan level 2 (managed process), dengan nilai persentase PA 2.1 sebesar 68,33% dan PA 2.2 sebesar 67,5%, berkategori L (largely achieved). Dengan ini menjelaskan bahwa sebagian besar tindakan proses APO13 pada level 2 telah diterapkan dan dikelola dengan tepat.

### 4.4. Finding and Recommendation

Rekomendasi berdasarkan temuan dan hasil penilaian pada proses APO12 yaitu memeriksa dengan teliti dan mencatat langkah-langkah

yang diperlukan untuk mengurangi risiko yang dihadapi; mengidentifikasi, mengendalikan, dan meninjau produk kerja secara berkala; menyediakan serta menetapkan infrastruktur yang memadai untuk meningkatkan efisiensi dalam pelaksanaan proses manajemen risiko; menyusun dokumen tertulis yang menjelaskan analisis Cost Benefit untuk memperkirakan potensi kerugian dan keuntungan dalam menangani skenario risiko; memberikan instruksi khusus kepada semua individu yang bertanggung jawab atas manajemen risiko keamanan informasi melalui sesi pelatihan khusus.

Rekomendasi berdasarkan temuan dan hasil penilaian pada proses APO13 yaitu menyiapkan atau menugaskan staf terkait untuk mengikuti sosialisasi atau acara terkait audit sistem guna memperoleh sertifikasi dan manajemen yang terkait dengan audit internal; melakukan peninjauan terhadap efektivitas pengelolaan Sistem Manajemen Keamanan Informasi (SMKI) dari hasil rekomendasi audit eksternal atau evaluasi yang berkaitan dengan keamanan informasi, serta meninjau hasil tersebut untuk memberikan saran perbaikan terkait SMKI untuk organisasi di masa depan; melakukan penyesuaian kinerja proses dengan melibatkan tindakan seperti mengidentifikasi masalah kinerja dan menyesuaikan rencana serta jadwal jika kinerja yang direncanakan tidak tercapai.

Rekomendasi berdasarkan temuan dan hasil penilaian pada proses DSS05 yaitu membuat skala prioritas dan mengoordinasikan pelaksanaan penetration testing serta mengelola biaya yang terkait; melakukan pengecekan atau meninjau akun atau hak akses serta mengevaluasi audit atau evaluasi terkait hak akses terhadap informasi yang sensitif; menyusun dokumen tertulis yang menjelaskan prosedur pencatatan dan perubahan hak akses serta kebijakan pembatasan akses ke situs TI; menyusun dan menetapkan dokumen prosedur untuk mengelola penerimaan, pemindahan, pemusnahan, penggunaan, dan pembuangan dokumen sensitif di dalam atau di luar organisasi.

## 5. KESIMPULAN

Berdasarkan hasil evaluasi tingkat kemampuan manajemen risiko keamanan informasi terhadap Dinas Komunikasi dan Informatika Kabupaten Lamongan, didapatkan

nilai proses APO12 sebesar 56.27% dengan kategori L (largely achieved) berada pada level 1, APO13 sebesar 68.33% (PA 2.1) dan 67.5% (PA 2.2) dengan kategori L (largely achieved) berada di level kedua, serta proses DSS05 sebesar 69.13% dengan kategori L (largely achieved) berada pada level 1. Dimana sebagian besar dari proses APO12 dan DSS05 telah dijalankan dan sebagian besar dari pencapaiannya didukung oleh bukti yang cukup. Sementara itu, pada level 2, terdapat satu proses dalam proses APO13 yang sudah diterapkan dan dikelola dengan tepat.

Saran perbaikan dan rekomendasi untuk Dinas Komunikasi dan Informatika Kabupaten Lamongan adalah menimbang serta menerapkan rekomendasi dan perbaikan pada proses APO12 mengelola risiko, APO13 mengelola keamanan, dan DSS05 mengelola layanan keamanan. Hal ini tujuannya adalah untuk menjamin bahwa semua pemangku kepentingan memiliki pemahaman yang kuat tentang elemen tertentu., dengan mendefinisikan dan mengkomunikasikan praktik kerja secara jelas. Selain itu, untuk penelitian selanjutnya, disarankan untuk menyusun produk kerja yang belum terpenuhi dan mengevaluasi tingkat kapabilitas dengan menggunakan proses TI lainnya dalam kerangka kerja COBIT 5.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada teman-teman, dosen pembimbing, serta staff Dinas Komunaikasi dan Informatika Kabupaten Lamongan yang telah memberi dukungan dan kontribusi terhadap penelitian ini.

## DAFTAR PUSTAKA

- [1] A. Hanif, M. Giatman, and A. Hadi, "Evaluasi Tata Kelola Teknologi Informasi Di Dinas Komunikasi Dan Informatika Menggunakan Framework COBIT," *J. Sains dan Teknol.*, vol. 9, no. 1, pp. 94–101, 2020.
- [2] A. K. Darmawan and A. Dwiharto, "Pengukuran Capability Level Kualitas Layanan E-Government Kabupaten Pamekasan Menggunakan Framework COBIT 5.0," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 3, no. 2, p. 93, 2019, doi: 10.29407/intensif.v3i2.12659.
- [3] S. Mukaromah, Z. F. Chairunnisa, A. Pratama, A. B. Putra, and P. M. Kusumantara, "Pengukuran Maturity Level Untuk Tujuan

- Bisnis 10 Meningkatkan Fungsionalitas Proses Bisnis,” *SCAN - J. Teknol. Inf. dan Komun.*, vol. 16, no. 1, pp. 1–5, 2021, doi: 10.33005/scan.v16i1.2476.
- [4] M. F. A. Effendi, A. R. Perdanakusuma, and B. T. Hanggara, “Evaluasi Kapabilitas Keamanan Teknologi Informasi pada Proses APO13 dan DSS05 berdasarkan Framework COBIT 5 (Studi pada Dinas Komunikasi dan Informatika Kota Malang),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 2, pp. 698–708, 2020.
- [5] S. Mukaromah *et al.*, “Alignment of Business Goals With IT Goals By Measuring The Level of Capability Using Cobit 5,” *Proceeding - IEEE 8th Inf. Technol. Int. Semin. ITIS 2022*, pp. 354–358, 2022, doi: 10.1109/ITIS57155.2022.10010265.
- [6] J. J. S. Peña, E. F. Vicente, and A. M. Ocaña, “ITIL, COBIT and EFQM: Can They Work Together?,” *Int. J. Comb. Optim. Probl. Informatics*, vol. 4, no. 1, pp. 54–64, 2010, [Online]. Available: <http://www.redalyc.org/articulo.oa?id=265225625006>
- [7] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.
- [8] D. Darmawan and A. F. Wijaya, “Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ,” *J. Comput. Inf. Syst. Ampera*, vol. 3, no. 1, pp. 1–17, 2022, doi: 10.51519/journalcisa.v3i1.139.
- [9] L. D. Fitriani and R. V. H. Ginardi, “Analysis Improvement of Helpdesk System Services Based on Framework COBIT 5 and ITIL 3rd Version (Case Study: DSIK Airlangga University),” *IPTEK J. Proc. Ser.*, vol. 0, no. 1, p. 28, 2019, doi: 10.12962/j23546026.y2019i1.5102.
- [10] E. Ekowansyah, Y. H. Chrisnanto, Puspita, and N. Sabrina, “Audit sistem informasi akademik menggunakan COBIT 5 di Universitas Jenderal Achmad Yani,” *Pros. Semin. Nas. Komput. dan Inform.*, vol. 2017, pp. 201–205, 2017.
- [11] D. Sanjaya and F. M. Indah, “Measurement of Capability Level Using COBIT 5 Framework (Case Study: PT Andalan Bunda Bijak),” *Ultim. Infosys J. Ilmu Sist. Inf.*, vol. 13, no. 2, pp. 715–721, 2022, doi: 10.33379/gtech.v7i2.2396.
- [12] F. Greene, “Selected COBIT 5 Processes for Essential Enterprise Security,” *Isaca*, pp. 1–3, 2015.
- [13] Y. Megasyah and A. A. Arifnur, “Academic Information System Security Audits Using Cobit 5 Framework Domains Apo12, Apo13 and Dss05,” *J. Appl. Eng. Technol. Sci.*, vol. 1, no. 2, pp. 124–135, 2020, doi: 10.37385/jaets.v1i2.79.
- [14] Inayatulloh, *Manajemen Risiko dan Audit Sistem Infomasi*. Universitas Terbuka, 2021. [Online]. Available: <https://pustaka.ut.ac.id/lib/msim4305-manajemen-risiko-dan-audit-sistem-infomasi/#tab-id-4>
- [15] A. Arief and I. H. A. Wahab, “Information Technology Audit For Management Evaluation Using COBIT and IT Security,” *2016 3rd Int. Conf. Inf. Technol. Comput. Electr. Eng.*, pp. 388–392, 2016.
- [16] S. Humaira, G. F. Nama, and R. A. Pradipta, “Analisis Tata Kelola Teknologi Informasi Menggunakan Cobit 5 Subdomain Dss01 Manage Operations (Studi Kasus: PT . BRI BO LIWA),” *JITET (Jurnal Inform. dan Tek. Elektro Ter.)*, vol. 12, no. 2, pp. 1408–1415, 2024.
- [17] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim),” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.
- [18] K. Budiarta, A. P. Saputra Iskandar, and M. Sudarma, “Audit Information System Development using COBIT 5 Framework (case Study: STMIK STIKOM Bali),” *Int. J. Eng. Emerg. Technol.*, vol. 1, no. 1, pp. 3–7, 2020, doi: 10.4108/eai.11-12-2019.2290885.
- [19] ISACA, *COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT*. ISACA, 2012.
- [20] ITGID, “Mengenal COBIT, Pengertian, Tujuan dan Pelatihan - ITGID | IT Governance Indonesia,” 2022. <https://itgid.org/mengenal-cobit-pengertian-tujuan-dan-pelatihan/> (accessed Nov. 23, 2023).
- [21] ISACA, *Process Assessment Model (PAM) : Using COBIT 5*. ISACA, 2013.
- [22] ISACA, *Self Assessment Guide: Using COBIT 5*. ISACA, 2013.
- [23] C. L. Prasetyo and S. Mukaromah, “Perancangan Alat Ukur Tingkat Kapabilitas Manajemen Risiko Keamanan Informasi Berdasarkan COBIT 5,” *SCAN - J. Teknol. Inf. dan Komun.*, vol. XVI, pp. 42–46, 2021.