

## **PENGUKURAN TINGKAT KAPABILITAS MANAJEMEN RISIKO KEAMANAN INFORMASI PADA SEKSI PERSANDIAN MENGUNAKAN COBIT 5**

### **MEASUREMENT OF INFORMATION SECURITY RISK MANAGEMENT CAPABILITY LEVEL IN SEKSI PERSANDIAN USING COBIT 5**

**Nur Ulfa Mauludina<sup>1\*</sup>, Siti Mukaromah<sup>1</sup>, Anita Wulansari<sup>1</sup>**

\*E-mail: [1\)19082010093@student.upnjatim.ac.id](mailto:119082010093@student.upnjatim.ac.id)

<sup>1</sup>Sistem Informasi, Fakultas Ilmu Komputer, UPN Veteran Jawa Timur

#### **Abstrak**

Penerimaan teknologi informasi dalam suatu organisasi dapat menjadi sarana yang akan membantu dalam menyaring sebuah informasi sebagai alat bantu untuk menjalankan proses bisnis organisasi. Informasi yang dihasilkan sebaiknya dapat dipercaya dan sesuai dengan keadaan yang sebenarnya. Penyelesaian masalah dengan menggunakan teknologi informasi tersebut tidak menutup kemungkinan akan memunculkan berbagai risiko yang akan dijumpai. Dinas Komunikasi dan Informatika Kabupaten Sumenep merupakan salah satu Satuan Kerja (SatKer) di lingkungan pemerintahan Kabupaten Sumenep yang memiliki tanggung jawab dalam pelaksanaan urusan pemerintahan di bidang informasi dan komunikasi publik, teknologi informatika serta statistik dan persandian. Dalam pelaksanaan tugasnya seksi persandian melakukan proses bisnis untuk memberi perlindungan informasi melalui Penyediaan Perangkat Teknologi Keamanan Informasi dan Jaring Komunikasi Sandi (JKS) serta melaksanakan pengiriman, menyimpan, hingga menghancurkan informasi yang bersifat umum dan rahasia. Penelitian ini mengukur 2 proses pada COBIT 5, yakni EDM03 *Ensure Risk Optimisation* dan APO12 *Manage Risk*. Hasil penilaian menunjukkan bahwa proses EDM03 dan APO12 berada pada level 1 (*Performed*) dan mempunyai nilai kesenjangan sebesar 3 dari level yang diharapkan yaitu 4 (*Predictable*). Nilai kesenjangan diperoleh dari selisih antara level yang diinginkan dan level yang dicapai saat ini dalam mencapai kapabilitas.

**Kata kunci:** *informasi, risiko, keamanan, seksi persandian, cobit 5*

#### **Abstract**

*Acceptance of information technology in an organization can be a tool that will assist in filtering information as a tool to run the organization's business processes. The information generated should be reliable and in accordance with the actual situation. Solving problems using information technology does not rule out the possibility of various risks that will be encountered. The Sumenep Regency Communication and Informatics Office is a work unit within the Sumenep Regency administration which has responsibility for implementing government affairs in the fields of public information and communication, informatics technology and statistics and coding. In carrying out its duties the encryption seksi persandian carries out business processes to provide information protection through Provision of Information Security Technology Devices and Password Communication Network as well as carrying out sending, storing, and destroying information that is both public and confidential. This study measures 2 processes in COBIT 5, namely EDM03 *Ensure Risk Optimization* and APO12 *Manage Risk*. The results of the assessment show that the EDM03 and APO12 processes are at level 1 (*Performed*) and have a gap value of 3 from the expected level of 4 (*Predictable*). The gap value is obtained from the difference between the desired level and current level achieved in achieving capability.*

**Keywords:** *information, risk, security, seksi persandian, COBIT 5*

## 1. PENDAHULUAN

Saat ini penggunaan teknologi informasi merupakan kebutuhan primer yang tidak hanya selalu ada, melainkan hal yang harus diperhatikan dalam suatu organisasi. Penerimaan teknologi informasi dalam suatu organisasi dapat menjadi sarana yang akan membantu dalam menyaring sebuah informasi sebagai alat bantu untuk menjalankan proses bisnis organisasi. Informasi yang dihasilkan sebaiknya dapat dipercaya dan sesuai dengan keadaan yang sebenarnya. Karena informasi tersebut bisa dimanfaatkan sebagai kepentingan pribadi, bisnis, lingkup pemerintahan, sekaligus dapat digunakan sebagai bahan untuk mengambil keputusan [9]. Penyelesaian masalah dengan menggunakan teknologi informasi tersebut tidak menutup kemungkinan akan memunculkan berbagai risiko yang akan dijumpai. Dengan risiko yang muncul tersebut akan membuat kurang optimalnya proses kerja, penurunan kualitas hingga minimnya pencapaian tujuan organisasi [10].

Dinas Komunikasi dan Informatika Kabupaten Sumenep merupakan salah satu Satuan Kerja (SatKer) di lingkungan pemerintahan Kabupaten Sumenep yang memiliki tanggung jawab dalam pelaksanaan urusan pemerintahan di bidang informasi dan komunikasi publik, teknologi informatika serta statistik dan persandian. Setiap proses bisnis yang dilakukan pada setiap bidang di Diskominfo Kabupaten Sumenep membutuhkan keamanan informasi, sehingga membutuhkan satu bidang yang memegang tanggungjawab dalam penyelenggaraan kebijakan atas keamanan informasi instansi dan pemerintah daerah yaitu oleh seksi persandian pada bidang statistik dan persandian. Dalam pelaksanaan tugasnya seksi persandian melakukan proses bisnis untuk memberi perlindungan informasi melalui Penyediaan Perangkat Teknologi Keamanan Informasi dan Jaring Komunikasi Sandi (JKS) serta melaksanakan pengiriman, menyimpan, hingga menghancurkan informasi yang bersifat umum dan rahasia. Informasi yang diterima berupa surat masuk yang berasal dari pusat (Presiden, Kementerian, Kedutaan besar luar negeri, dan dinas terkait di Provinsi Jawa Timur maupun luar provinsi yang kemudian akan di distribusikan menyesuaikan tembusan surat didalamnya (Bupati/wakil, Sekretaris Daerah, dinas dan kecamatan terkait di lingkungan Pemerintah Kabupaten Sumenep, dsb. Dari pelaksanaan tersebut selanjutnya akan disusun kebijakan teknis terkait keamanan informasi, terutama di lingkungan pemerintah daerah Kabupaten Sumenep.

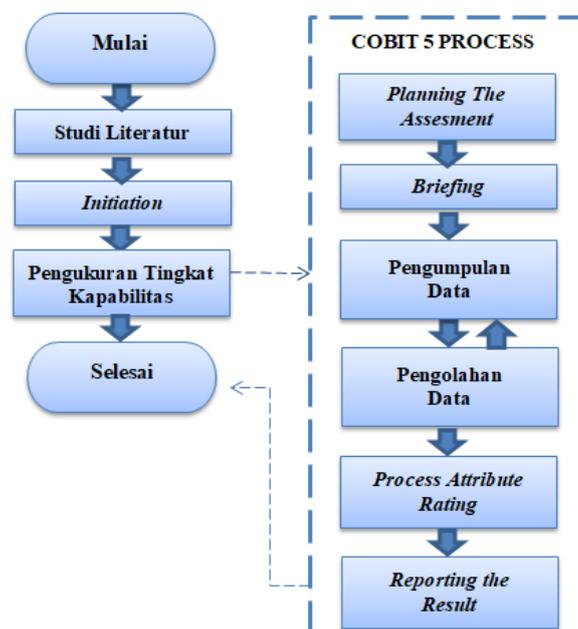
Dalam pelaksanaan tugas kerjanya, seksi persandian yang memiliki fungsi untuk menyusun peraturan teknis operasional pengamanan komunikasi sandi yang dimana belum dilakukan evaluasi dan diberikan standar terkait keamanan informasinya sehingga dapat menimbulkan beberapa risiko keamanan yang dapat terjadi seperti masalah terkait kehilangan atau kerusakan dalam penyimpanan data *online* yang masuk ke dalam sistem informasi pendataan internalnya yang disebabkan oleh peretasan pihak yang tidak dikenal maupun terjadinya hal yang menyebabkan aset informasi yang bersifat rahasia dapat tersebar ke lingkungan luar persandian. Sehingga perlu dilakukan pengukuran untuk meminimalisir potensi risiko terkait pengiriman dan pertukaran informasi khususnya yang bersifat rahasia. Evaluasi terkait Diskominfo Kabupaten Sumenep juga dilaksanakan agar diketahui sejauh mana instansi menerapkan manajemen risiko keamanan informasinya

Dari uraian tersebut, dibutuhkan sebuah standar *base practice* yang perlu dilakukan dalam penerapan sebagai pedoman untuk melakukan pengukuran kapabilitas, hal ini bertujuan untuk memberikan analisis optimalisasi terkait manajemen risiko keamanan informasi serta dapat meminimalisasi potensi risiko dalam pengiriman dan pertukaran aset dan dokumen, terutama untuk penyampaian informasi yang bersifat rahasia atau sensitif sehingga dapat dilakukan pencegahan agar tidak terjadinya penyebaran informasi yang dapat menghambat proses bisnis kinerja seksi persandian Diskominfo Kabupaten Sumenep. Terdapat beberapa standarisasi yang dapat dilakukan dalam pengelolaan TI seperti COBIT, ITIL, ISO/IEC 270001 dan setiap standar tersebut dapat digunakan dan dikelola dalam berbagai kondisi tertentu [7].

Beberapa penelitian sebelumnya dengan permasalahan yang sama tentang manajemen risiko keamanan informasi, banyak yang menerapkan COBIT 5 sebagai acuan kerangka kerjanya. Berdasarkan penelitian pada tahun 2018, pengevaluasian terkait manajemen risiko teknologi informasi dilakukan oleh Riyan untuk mengukur dan mengetahui cara meminimalisir berbagai risiko dan mencegah adanya kesalahan pada PT Taspen. Fokus penelitian menggunakan domain proses EDM03 dan APO12 dari hasil penghitungan di dapatkan nilai kapabilitas berada pada level 1 yang dimana PT Taspen telah melakukan pengimplementasian terkait manajemen risiko namun belum dioptimalisasi [10]. Pada tahun yang sama pula, Arief melakukan pengukuran terkait kapabilitas pada Perum Jasa Tirta I Malang dengan menggunakan domain proses EDM03 dan APO12. Dimana keduanya memperoleh nilai kapabilitas pada level 2, yaitu jika pengimplementasian telah dikelola dengan baik dan hasil pekerjaan tetap terpantau dan terkelola dengan tepat. Hasil gap yang telah dibentuk untuk masing-masing domain proses adalah sebesar 1[4].

## 2. METODOLOGI

Dalam penelitian ini digunakan tahapan untuk menyelesaikan permasalahan, yang dipaparkan pada **Gambar 1** berikut:



**Gambar 1. Tahapan Penelitian**

### 2.1 Studi Literatur

Pada langkah pertama penelitian dibutuhkan beberapa data dan informasi yang dapat diperoleh dari sumber terkait, serta dokumentasi dari penelitian yang telah dilakukan sebelumnya. Dalam tahap ini selain untuk menyusun kerangka penelitian juga bertujuan untuk memperoleh data penelitian dengan memanfaatkan beberapa sumber pustaka yang terkait evaluasi manajemen risiko keamanan informasi menggunakan kerangka kerja COBIT 5 dan dimulai dengan mengumpulkan teori dasar tentang COBIT 5 dan manajemen keamanan informasi. Adapun data dan informasi yang telah diperoleh diharapkan akan membantu dalam melakukan pengukuran tingkat kapabilitas manajemen keamanan informasi.

### 2.2 Initiation

Tujuan pada tahap ini adalah untuk memberikan penjelasan mengenai hasil data dan informasi yang telah terkumpul. *Value* dimunculkan oleh berbagai *stakeholder* yang terlibat dalam suatu organisasi. Semua *stakeholder* sebaiknya dipertimbangkan oleh sistem dari tata kelola dalam membuat keputusan terkait penilaian manfaat, risiko, dan sumber daya. *Stakeholder needs* memiliki 3 fokus utama yaitu *benefits realisation*, *risk optimisation* dan *resource optimization*. Dengan menyesuaikan kebutuhan Seksi Persandian dari Diskominfo Kabupaten Sumenep yang menjadi studi kasus dalam skripsi ini membutuhkan pengoptimalan dalam manajemen risiko yang berkaitan dengan keamanan informasi karena seksi tersebut yang memegang kendali atas keamanan TI dan urgensi terkait proses bisnis utamanya. Pemetaan dilakukan dengan menentukan P (*Primary*) tujuan bisnis instansi ke dalam COBIT 5 pada *Enterprise Goals* yang sesuai dengan kondisi instansi.

Tahapan pemetaan domain proses diawali dengan memberikan beberapa pertanyaan terkait *stakeholder needs* pada narasumber dan pertanyaan yang diperoleh dari wawancara awal yaitu “*Is the information I am processing well secured?*” hal ini karena seksi persandian memiliki tugas dan fungsi yang berkaitan dengan keamanan sehingga perlu diketahui proses implementasinya. Kemudian dilanjutkan dengan menentukan *Enterprise Goal* pada seksi persandian yaitu untuk mengetahui terkait presentase kebijakan yang didukung oleh standar dan praktik kerja yang efektif terkait manajemen risiko keamanan informasi.

**Figure 24—Mapping COBIT 5 Enterprise Goals to Governance and Management Questions (cont.)**

STAKEHOLDER NEEDS	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
	Stakeholder value of business investments																
Portfolio of competitive products and services																	
Managed business risk (mitigating of assets)																	
Compliance with external laws and regulations																	
Financial transparency																	
Customer-oriented service culture																	
Business service continuity and availability																	
Able responses to a changing business environment																	
Information-based strategic decision making																	
Optimisation of service delivery costs																	
Optimisation of business process functionality																	
Optimisation of business process costs																	
Managed business change programmes																	
Operational and staff productivity																	
Compliance with internal policies																	
Skilled and motivated people																	
Product and business innovation culture																	
<b>Is the information I am processing well secured?</b>																	
<b>How do I improve business agility through a more flexible IT environment?</b>																	

Gambar 2. Pemetaan Tujuan Bisnis pada Tujuan TI

IT related goal	Learning Goals																
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
01 Alignment of IT and business strategy																	
02 IT compliance and support for business compliance with external laws and regulations																	
03 Commitment of executive management for making IT-related decisions																	
04 Managed benefits from IT-enabled investments and services portfolio																	
05 Transparency of IT costs, benefits and risk																	
06 Delivery of IT services in line with business and technology solutions																	
07 Adequate use of applications, information and technology solutions																	
08 IT agility																	
09 Security of information, processing infrastructure and applications																	
10 Optimisation of IT assets, resources and processes by integrating applications and technology into business processes																	
11 Enablement and support of business processes by integrating applications and technology into business processes																	
12 Delivery of reliable and useful information to stakeholders meeting requirements and quality standards																	
13 Availability of reliable and useful information for decision making																	
14 Availability of reliable and useful information for decision making																	
15 IT compliance with internal policies																	
16 IT compliance with internal policies and staff productivity																	
17 Knowledge, expertise and initiatives for business innovation																	

Gambar 3. Pemetaan Enterprise Goals pada IT Related Goals

### 2.3 Planning the Assessment

Pada tahapan kedua ini dilakukan perencanaan penilaian yang bertujuan untuk mendapatkan hasil evaluasi dari penilaian tingkat kapabilitas. Tahap ini meliputi pemetaan RACI Chart

menyesuaikan dengan tugas fungsional instansi agar selaras dengan kebutuhan kegiatan penilaian.

Fungsional yang akan menjadi auditee pada penelitian ini hanya pada peran R (*Responsible*), dikarenakan peran tersebut yang memiliki tanggung jawab secara langsung dalam setiap kegiatan TI dan peran tersebut merupakan jabatan yang paling tinggi dalam instansi. Adapun auditee dari kedua proses ini akan dilakukan wawancara kepada Kepala Bidang Statistik Persandian dan Sandiman Ahli Muda pada Dinas Komunikasi dan Informatika Kabupaten Sumenep.

#### 2.4 Briefing

Dalam tahap ini akan dilakukan diskusi dan memberikan pemahaman terkait proses penelitian untuk skripsi kepada para auditee Diskominfo Kabupaten Sumenep agar dapat memahami akan beberapa proses dalam pengukuran tingkat kapabilitas dan dokumen yang akan dibutuhkan dalam proses penilaian.

#### 2.5 Pengumpulan Data

Tahapan selanjutnya adalah dengan mengumpulkan dokumen dari hasil yang telah diperoleh dari wawancara kepada auditee. Pengumpulan data bertujuan untuk memperoleh bukti pendukung dari pernyataan auditee sebagai evaluasi penilaian pada proses yang dilakukan

#### 2.6 Pengolahan Data

Pada tahap ini memastikan kecukupan dan akurasi dari dokumen yang telah dikumpulkan dengan auditee sesuai dengan RACI Chart. Dalam tahapan ini dan sebelumnya dapat berjalan bersamaan dikarenakan dimana jika masih terdapat kekurangan data maka akan kembali kepada tahap sebelumnya. Sekaligus untuk memastikan kembali terkait kebenaran data yang diperoleh.

Pengolahan data dilakukan dengan 2 tahapan, yaitu wawancara dan validasi dokumen. Wawancara dilakukan dengan auditee yang telah dipilih menggunakan RACI *Chart*. Dalam wawancara mengulik beberapa informasi terkait studi kasus serta untuk memperoleh bukti pendukung berupa dokumen yang akan membantu dalam proses penilaian. Validasi dilakukan oleh penulis terhadap proses bisnis yang telah diamati. Jika dokumen yang disampaikan tidak sesuai dengan kebenaran yang ada, maka dilakukan peninjauan ulang hingga dokumen yang ada sesuai dengan realitas saat melakukan wawancara kepada auditee.

#### 2.7 Process Attribute Rating

Proses pengukuran tingkat kapabilitas akan dilaksanakan pada tahapan ini dengan menyesuaikan hasil temuan melalui wawancara dan pengumpulan dokumen. Tingkat kapabilitas setiap proses dihitung berdasarkan 2 jenis indikator penilaian yaitu dengan menggunakan indikator atribut kapabilitas pada tingkat kapabilitas 1-5 dan indikator kinerja pada tingkat kapabilitas 1 secara eksklusif.

Pengukuran tingkat kapabilitas didasarkan pada skor *outcomes* dan skor produk kerja. *Base practice* (BP) menyediakan definisi tugas dan aktivitas untuk menyelesaikan tujuan dari proses dan memenuhi *outcome* yang berupa acuan pertanyaan dan *work product* dari domain yang dipilih. Skor *outcome* akan menjadi penentu dalam tingkat kapabilitas level 1 sedangkan level 2 sampai selanjutnya akan dilakukan dengan menilai temuan GP dan GWP yang kemudian akan diberi kategori dengan rating dengan skala N-P-L-F seperti tabel 1 berikut:

Tabel 1. Tabel Skala Rating

Rating	Nilai	Deskripsi
N	0-15%	Terdapat sedikit atau tidak adanya bukti capaian dari proses atribut.
P	>15-50%	Terdapat bukti dari pendekatan sistematis dan beberapa capaian.
L	>50-85%	Terdapat bukti dari pendekatan sistematis dan capaian yang signifikan.
F	>85%-100%	Terdapat bukti yang lengkap dan penuh

capaian dan tidak terdapat kelemahan.

Berikut perhitungan *base practice* yang diperoleh dari hasil persamaan 1 dan 2.

$$\text{Nilai Base Practice} = \frac{\sum \text{skorBP}}{\sum \text{totalBP}} \times 100\% \dots\dots\dots (1)$$

$$\text{Nilai Work Product} = \frac{\sum \text{WP}}{\sum \text{totalWP}} \times 100\% \dots\dots\dots (2)$$

### 2.8 Reporting The Result

Setelah mendapatkan hasil akhir pengukuran tingkat kapabilitas, selanjutnya akan memberikan pelaporan kepada Seksi Persandian Diskominfo Kabupaten Sumenep atas hasil temuan dan evaluasi pada setiap proses.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Process Attribute Rating

Berikut merupakan hasil penilaian terhadap *base practice* dan *work product* proses EDM03 dan APO12.

**Tabel 2. Tabel Penilaian BP EDM03**

Tujuan Proses	Skor
EDM03.01	50%
EDM03.02	64%
EDM03.03	71%
<b>Rata-Rata</b>	<b>62%</b>

**Tabel 3. Tabel Penilaian BP APO12**

Tujuan Proses	Skor
APO12.01	47%
APO12.02	86%
APO12.03	49%
APO12.04	39%
<b>Rata-Rata</b>	<b>55%</b>

Secara garis besar berdasarkan hasil penilaian kedua proses optimasi manajemen risiko telah dilakukan dengan baik. Penentuan dan penilaian terkait risiko telah dilakukan dan dipantau dengan rutin untuk memastikan penanganannya terkendali. Skor diperoleh dari beberapa temuan proses salah satunya adalah terdapat beberapa praktik yang belum terlaksana dengan baik untuk mengidentifikasi peristiwa risiko. Dengan demikian kedua proses EDM03 dan APO12 masih berada pada level L (*Largely Achieved*).

**Tabel 4. Tabel Penilaian WP EDM03**

Praktik Dasar	Skor
EDM03.01	100%
EDM03.02	100%
EDM03.03	100%
<b>Rata-Rata</b>	<b>100%</b>

**Tabel 5. Tabel Penilaian WP APO12**

Praktik Dasar	Skor
---------------	------

APO12.01	100%
APO12.02	100%
APO12.03	100%
APO12.04	67%
APO12.05	0%
APO12.06	100%
<b>Rata-Rata</b>	<b>78%</b>

Berdasarkan total rata-rata dari skor tujuan proses dan skor produk kerja, maka selanjutnya akan dilakukan perhitungan dari keseluruhan skor dari proses EDM03 dan APO12.

$$\begin{aligned}
 \text{Skor Proses EDM03} &= \frac{\text{Outcomes} + \text{WP}}{2} \times 100\% \\
 &= \left( \frac{69 + 100}{2} \right) \% \\
 &= 81\% \qquad (3)
 \end{aligned}$$

$$\begin{aligned}
 \text{Skor Proses APO12} &= \frac{\text{Outcomes} + \text{WP}}{2} \times 100\% \\
 &= \left( \frac{55 + 78}{2} \right) \% \\
 &= 67\% \qquad (4)
 \end{aligned}$$

Berdasarkan hasil penrhitungan dapat diperoleh skor proses EDM03 dan APO12 sebesar 81% dan 67% yang tergolong dalam kategori skor L (*Largely Achieved*). Dan dengan demikian kedua proses hanya sampai pada level 1 *Performed*.

### 3.2 Reporting The Result

Pada tahapan ini berisi rekapitulasi hasil pengukuran kapabilitas dari proses EDM03 dan APO12. Juga terdapat nilai kesenjangan antara level harapan dan saat ini telah dicapai,

**Tabel 6. Analisa Kesenjangan**

Proses	Penilaian Level	Level Saat ini	Level Harapan
EDM03	81% L	1	4
APO12	67% L	1	4
<b>Kesenjangan</b>			<b>3</b>

Berdasarkan hasil pengukuran tingkat kapabilitas manajemen risiko keamanan informasi Seksi Persandian Diskominfo Kabupaten Sumenep, pada proses EDM03 dan APO12 berada pada kategori L (*Largely Achieved*) dengan masing-masing mendapatkan nilai sebesar 81% dan 67%. Dengan demikian, kedua proses tersebut masih berada pada level 1 (*Performed*) dimana pada level ini proses yang diimplementasikan telah mencapai tujuan prosesnya.

Dari hasil pengukuran Dinas Komunikasi dan Informatika Kabupaten Sumenep memiliki level harapan 4 (*Predictable Process*). Dimana level ini ditentukan berdasarkan hasil wawancara dengan Kepala Bidang Seksi dan Persandian dan Sandiman Ahli Muda. Berdasarkan tabel 5

pada kedua proses EDM03 dan APO12 memiliki nilai kesenjangan sebesar 3 level. Nilai kesenjangan dapat dilakukan sebagai acuan dasar untuk menyusun langkah-langkah perbaikan untuk dapat mencapai level harapan yang diinginkan.

#### 4. KESIMPULAN DAN SARAN

Hasil pengukuran mengenai penerapan manajemen risiko keamanan informasi pada Seksi Persandian Dinas Komunikasi dan Informatika Kabupaten Sumenep menggunakan kerangka kerja COBIT 5 dengan domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*) menghasilkan penilaian kapabilitas yang berada pada level 1 atau *Performed*, dimana hasil tersebut menunjukkan jika Dinas Komunikasi dan Informatika Kabupaten Sumenep berada pada tahap implementasi manajemen risiko keamanan informasi. Analisis kesenjangan diperoleh dari selisih antara level harapan dan saat ini yaitu level 4 (*Predictable*) dengan level kapabilitas yaitu level 1 (*Performed*) saat ini pada proses EDM03 dan APO12 sebesar 3.

Saran untuk penelitian selanjutnya adalah, dapat melakukan pengukuran pada proses APO13 (*Managed Security*) dan BAI06 (*Managed Changes*) yang merupakan proses terpilih dari pemetaan yang dilakukan pada skripsi ini yang juga merupakan proses yang berhubungan dengan manajemen risiko. Dan dapat melakukan pengukuran menggunakan kerangka kerja selain COBIT 5 yang fokus pada manajemen risiko keamanan informasi sebagai perbandingan hasil penilaian untuk meninjau tindak perbaikan yang dibutuhkan.

#### 5. DAFTAR RUJUKAN

- [1] ISACA. 2012. *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT Using COBIT 5*. USA:ISACA.
- [2] ISACA. 2012. *COBIT 5 Enabling Process*. USA:ISACA.
- [3] Agtika, A. S., Mursityo, Y. T., & Rachmadi, A., 2019, Evaluasi Manajemen Risiko Teknologi Informasi pada Badan Perencanaan, Penelitian dan Pengembangan (Barenlitbang) Kota Malang Menggunakan Cobit 5 Domain EDM03 dan APO12, *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Vol. 3, No. 5, 4218-4225.
- [4] Arief, M.H., & Suprpto., 2018, Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang), *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Vol.2 No.1.
- [5] Budiono, N. J., Cahyono, A. D., & Tanaem, P. F., 2021, EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERUSAHAAN DAERAH AIR MINUM KOTA SALATIGA MENGGUNAKAN FRAMEWORK COBIT 5.0, Vol.35 No.1, 82-91.
- [6] Mukaromah, S. & Putra, A.B., 2016, Maturity level at university academic information system linking it goals and business goal based on COBIT 4.1, *MATEC Web Conf.*, vol. 58, 2016, , doi: 10.1051/mateconf/20165803009.
- [7] Mukaromah, S., Riesta, M.A., Prasetyo, L. C., Safitri, M. E., Kusumantara, M.P., Putra, B.A., et al., 2022, Alignment of Business Goals With IT Goals By Measuring The Level of Capability Using Cobit 5, *2022 IEEE 8th Information Technology International Seminar (ITIS)*, 354-358.
- [8] Prasetyo, C. L., & Mukaromah, S., 2021, PERANCANGAN ALAT UKUR TINGKAT KAPABILITAS MANAJEMEN RISIKO KEAMANAN INFORMASI BERDASARKAN COBIT 5, *SCAN*, Vol.XVI No 3, 42-46.
- [9] Riadi, F.T., Manuputty, A. D., & Saputra, A., 2018, Evaluasi Manajemen Risiko Keamanan Informasi dengan Menggunakan COBIT 5 Subdomain EDM03 (*Ensure Risk Optimisation*). *JUTEL*, vol. 2, no. 1, pp. 1–10, 2018, doi: 10.21460/jutei.2018.12.53.
- [10] Aziz, A.R., 2018, Evaluasi Manajemen Risiko Teknologi Informasi pada Perusahaan BUMN Menggunakan Standar COBIT 5 (Studi Kasus: PT Taspen Persero). *Jurnal IT CIDA*, Vol. 4, No.2. 1-11.

- [11] Setyaningrum, N.D. & Kusyanti, A., 2018, Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus : PT.Kimia Farma (Persero) Tbk – Plant Watudakon), vol. 2, no. 1, pp. 143–152.
- [12] Thenu, P. P., Wijaya, A. F., Rudianto, C., Kristen, U., & Wacana, S., 2020, Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus : Pt Global Infotech). *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13.
- [13] Utami, R. S., 2021, Pengukuran Tingkat Kapabilitas Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 dan Rekomendasi Perbaikan (Studi Kasus: Badan Pengembangan Teknologi Informasi), *Jurnal Ekonomi dan Manajemen Teknologi*, Vol.5 No.1, 31-36.
- [14] Wibawa, P. M., & Manuputty, A. D, 2020, Analisis Manajemen Risiko Teknologi Informasi Policy Service PT. Asuransi Sinar Mas Menggunakan Framework COBIT 5, *Jurnal Teknik Informatika dan Sistem Informasi*, Vol.7 No.3, 466-479.
- [15] Prasetyo, C. L, 2021. Pengukuran Kapabilitas Manajemen Risiko Keamanan Informasi pada Sistem Informasi Pengelolaan Surat Menggunakan Kerangka Kerja COBIT 5. Surabaya:UPN Veteran Jawa Timur.