PENGUKURAN TINGKAT KAPABILITAS MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN COBIT 5

MEASUREMENT OF INFORMATION SECURITY MANAGEMENT CAPABILITY LEVEL USING COBIT 5

Abiela Titan Susilo[1*], Siti Mukaromah[1], Eristya Maya Safitri[1]
*E-mail: [1)]19082010048@student.upnjatim.ac.id

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kediri yang berdasarkan Peraturan Bupati Nomor 33 Tahun 2019 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) Kabupaten Kediri memiliki wewenang penyelenggaraan *Government Chief Information Officer* (GCIO) Pemerintah Kabupaten yang berpotensi terhadap ancaman keamanan data. Sebagai tindakan preventif, tujuan penelitian ini untuk mengetahui tingkat kapabilitas keamanan informasi SPBE Diskominfo Kabupaten Kediri dengan proses yang diukur adalah APO13 *Manage Security* dan DSS05 *Manage Security Services.* Hasil perhitungan tingkat kapabilitas manajemen keamanan informasi pada Diskominfo Kabupaten Kediri pada proses APO13 mendapatkan skor 22,46% pada kategori P (*Partially Achieved)* sedangkan DSS05 mendapatkan skor yang lebih tinggi yaitu 70,47% pada kategori L (*Largely Achieved*). Dengan demikian, kedua proses pada level yang sama yaitu level 1 (*Performed*) yang menandakan pada level ini proses yang diimplementasikan mendekati atau mencapai tujuan prosesnya.
Kata kunci: *diskominfo, spbe, keamanan, kapabilitas, cobit 5.*

Abstract

The Kediri District Communication and Informatics Office (Diskominfo), based on Regent Regulation Number 33 of 2019 concerning the Kediri District Electronic-Based Government System (SPBE), has the authority to implement the District Government Chief Information Officer (GCIO) which has the potential for data security threats. As a preventive measure, the purpose of this study is to determine the level of information security capability of SPBE Diskominfo Kediri District with the measured processes are APO13 Manage Security and DSS05 Manage Security Services. The results of the calculation of the level of information security management capability at Diskominfo Kediri Regency in the APO13 process get a score of 22.46% in the P (Partially Achieved) category while DSS05 gets a higher score of 70.47% in the L (Largely Achieved) category. Thus, both processes are at the same level, namely level 1 (Performed) where at this level the implemented process approaches or achieves its process objectives.
Keywords*: diskominfo, spbe, security, capabilities, cobit 5.*

1. PENDAHULUAN

Data dan informasi merupakan objek utama yang tidak dapat dipisahkan dan merupakan sumber daya krusial yang perlu diperhatikan. Informasi menjadi suatu aset yang sangat penting dan berharga bagi keberlanjutan organisasi [1]. Selain itu, pentingnya informasi tersebut sehingga hanya beberapa orang tertentu yang dapat mengaksesnya. Pemilik informasi akan mengalami kerugian besar jika informasinya diketahui oleh pihak lawan bisnis [2]. Namun, banyaknya informasi akan berbanding lurus dengan tingginya ancaman keamanan informasi (*information security*). Keamanan informasi adalah upaya melindungi informasi terhadap segala ancaman untuk menetapkan keberlangsungan bisnis, memperkecil risiko bisnis, dan mencapai laba investasi dan peluang bisnis tertinggi [3]. Kerentanan informasi terhadap ancaman menjadi masalah kompleks bagi perusahaan, organisasi, hingga pemerintahan. Bahkan kelemahan kecil dalam sistem keamanan informasi dapat memiliki dampak negatif yang signifikan terhadap pencapaian tujuan perusahaan [4].

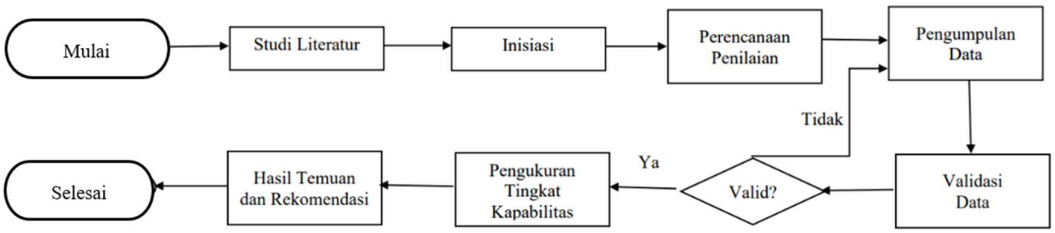
Sesuai Peraturan Bupati Nomor 33 Tahun 2019 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) Kabupaten Kediri menyebutkan bahwa "Setiap SKPD harus menerapkan Keamanan SPBE". Berdasarkan Peraturan Bupati Kediri Nomor 31 Tahun 2022 tentang kedudukan, susunan organisasi, uraian tugas dan fungsi serta tata kerja menyatakan bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri sebagai wali data memiliki kewenangan dalam perencanaan, perancangan, pembangunan, pengembangan, pengoperasian, dan evaluasi SPBE. Bidang Aplikasi Informatika memiliki wewenang untuk penyelenggaraan urusan layanan *disaster recovery center*, infrastuktur dasar *data center* & TIK, pelayanan keamanan informasi *e-Government*, pelayanan manajemen data dan informasi pada *e-Government*, hingga sebagai *Government Chief Information Officer* (GCIO) Pemerintah Kabupaten. Selain itu, Diskominfo Kabupaten Kediri pernah mengalami gangguan jaringan pada kantor kecamatan berdampak pada kendala pelayanan informasi pemerintahan dan proses pelaporan yang mengancam keamanan yang dikuatkan keterangan pada Buku 1 Kondisi Eksiting dan Analis GAP SPBE Pemerintah Kabupaten Kediri. Sebagai tindakan preventif, penelitian ini bertujuan untuk melaksanakan sebuah pengukuran tingkat kapabilitas keamanan informasi pada Diskominfo Kabupaten Kediri.

Pengukuran tingkat kapabilitas harus memiliki acuan *best practice* yaitu sebuah proses yang telah berhasil digunakan oleh perusahaan dan dapat menjadi contoh yang baik dari implementasi serupa di perusahaan lain. Beberapa *best practice* yang baik sebagai dasar untuk mengembangkan keamanan informasi dapat menggunakan COBIT dan ISO/IEC 27001 [5]. COBIT 5 adalah seperangkat praktik terbaik untuk manajemen teknologi informasi (TI) yang terdiri dari: rangkuman, kerangka kerja, tujuan pengendalian, pedoman audit, alat implementasi dan pedoman manajemen yang sangat berguna untuk sistem informasi yang strategis [6]. COBIT 5 bersifat umum yang dapat diimplementasikan di semua instansi, baik sektor publik atau pun komersial. COBIT 5 sendiri juga memiliki produk yang membahas secara khusus mengenai keamanan informasi yaitu COBIT 5 *for Information Security* [7]. Meskipun telah diterbitkan versi terbaru yaitu COBIT 2019 namun penelitian terkait COBIT 2019 sangat terbatas sehingga diputuskan menggunakan kerangka kerja COBIT 5 pada studi kasus ini.

Penelitian sebelumnya yang telah melakukan evaluasi pada Diskominfo Kabupaten Kediri dengan sudut pandang menggunakan indeks Keamanan Informasi mendapatkan hasil evaluasi level kesiapan dalam menerapkan standar ISO 27001 mencapai nilai "163" dalam area warna "Merah" yang berarti masih dalam kategori "Tidak Layak" untuk penerapan sertifikasi SNI ISO 27001:2013 [8]. Berdasarkan permasalahan pada Diskominfo Kabupaten Kediri, pengukuran tingkat kapabilitas keamanan informasi berfokus menggunakan kerangka kerja COBIT 5.

2. METODOLOGI

Pada penelitian ini menggunakan metodologi sesuai dengan alur pada gambar 1 berikut.



Gambar 1. Metodologi Penelitian

2.1 Studi Literatur

Tahap ini dilakukan penelusuran terhadap pustaka mengenai konsep tata kelola teknologi informasi, konsep keamanan informasi, dan teori mengenai COBIT 5 agar lebih memahami pengimplementasiannya dan dibutuhkan juga beberapa penelitian terdahulu dalam pengukuran tingkat kapabilitas manajemen keamanan informasi. Sumber pustaka berasal dari jurnal, buku, dan penelitian terdahulu. Seluruh literatur dirinci sesuai dengan lingkup penelitian.

2.2 Inisiasi

Inisiasi merupakan proses penetapan domain berdasarkan buku panduan COBT 5 *Enabling Process* dengan tujuan untuk mengidentifikasi proses apa saja yang akan diukur. Proses pemetaan dan penetapan domain dilakukan sesuai dengan tahapan COBIT 5 *Goals Cascade* yang disesuaikan dengan tujuan bisnis Dinas Komunikasi dan Informatika Kabupaten Kediri. Beberapa langkah pada tahapan ini terdiri dari menentukan *Stakeholder Needs* yaitu "*Is the information I am processing well secured?"* untuk dapat mengoptimasi risiko lalu dipetakan terhadap tujuan organisasi yang berfokus pada *enterprise goals* nomor 15 atau EG15 yaitu kepatuhan terhadapan kebijakan internal. Kemudian dipetakan dengan tujuan terkait TI nomor 10 yang berfokus tentang keamanan informasi, dan dipetakan proses COBIT 5. Pemetaan berdasarkan keterangan P *(Primary)* karena memiliki hubungan yang penting dan dapat mendukung tujuan atau proses tersebut [9].

2.3 Perencanaan Penilaian

Perencanaan penilaian digunakan untuk memetakan narasumber berdasarkan RACI *Chart* pada COBIT 5 guna mendapatkan informasi untuk pengukuran tingkat kapabilitas. Daftar narasumber berdasarkan pada RACI *Chart* berperan *Responsible* (R) yang memiliki tugas dan bertanggung jawab secara langsung melakukan pekerjaan lalu disesuaikan pada fungsi dan jabatan yang ada di Dinas Komunikasi dan Informatika Kabupaten Kediri [10]. Peran R dengan jabatan tertinggi dipilih sebagai narasumber sehingga informasi yang diterima valid [11].

2.4 Pengumpulan Data

Tahap ini dilakukan dengan mengumpulkan bukti objektif untuk memastikan terpenuhinya tingkat kapabilitas yang telah tercapai untuk setiap proses yang diukur sesuai COBIT 5. Bukti-bukti tersebut berupa seperangkat indikator kinerja proses spesifik untuk level 1 yang berisi *Base Practices* (BP) dan *Work Products* (WP) yang mendukung evaluasi proses terpilih. Pengumpulan data berupa pengidentifikasian produk kerja dari masing-masing proses yang telah tersedia pada COBIT 5.

2.5 Validasi Data

Tahap validasi dilakukan untuk untuk memeriksa hasil temuan dokumen yang ditunjukkan oleh narasumber sesuai proses domain yang terpilih untuk memastikan dokumen-dokumen tersebut akurat. Data didapatkan dari dua tahap yaitu tahap wawancara berdasarkan panduan COBIT 5 terkait proses atau kegiatan dasar yang telah dilaksanakan serta temuan di lapangan. Sedangkan memvalidasi bukti dokumen berfungsi untuk mendukung tercapainya proses dan sebagai objektivitas informasi yang dikumpulkan saat wawancara [12].

2.6 Pengukuran Tingkat Kapabilitas

Terdapat dua jenis indikator penilaian untuk menetapkan tingkat kapabilitas yang dijabarkan yaitu indikator kemampuan proses artibut yang terdiri dari *Generic Practice* (GP) dan *Generic Work Product* (GWP) dan bersifat generik untuk tiap atribut pada level 1 sampai level 5. Kedua yaitu indikator performa proses yang ekslusif digunakan untuk level 1 untuk mengetahui apakah sudah mencapai tujuan prosesnya dan dapat melanjutkan ke level yang lebih tinggi. Indikator performa proses sendiri terdiri dari praktik dasar/*base practice* (BP) dan produk kerja/*work products* (WP) yang khusus harus terpenuhi pada level 1 [12]. Perhitungan tingkat kapabilitas proses berdasarkan rata-rata skor keluaran/*outcomes* pada perhitungan (1) dan rata-rata skor produk kerja pada perhitungan (2) lalu dihitung untuk mengetahui skor keseluruhan proses pada perhitungan (3) [13].

$$Outcomes = \frac{\sum(\text{Skor Tujuan Proses})}{\text{Tujuan Proses}} \% \quad \ldots\ldots (1)$$

$$\text{Produk Kerja} = \frac{\sum(\text{Skor Produk Kerja})}{\text{Praktik dasar}} \% \quad \ldots\ldots (2)$$

$$\text{Skor Proses} = \frac{(Outcomes + \text{Produk Kerja})}{2} \% \quad \ldots\ldots (3)$$

Base practice atau praktik dasar telah mendefinisikan seperangkat aktivitas untuk memenuhi tujuan suatu proses sehingga *outcomes* proses tersebut dapat tercapai. Skor *outcomes* menjadi pertimbangan dalam penetapan tingkat kapabilitas pada level 1. Pada tingkat kapabilitas level 2 hingga seterusnya penilaian berdarkan pada *Generic Practice* (GP) dan *Generic Work Product* (GWP). Skor pada indikator dikelompokkan pada kategori skala N (*Not Achieved)*-P (*Partially Achieved*)-L (*Largelly Achieved*)-F (*Fully Achieved*) pada Tabel 1.

Tabel 1. Skala N-P-L-F

Skala	Skor
N	0% hingga 15%
P	15% hingga 50%
L	50% hingga 85%
F	85% hingga 100%

2.7 Hasil Temuan dan Rekomendasi

Pada tahap ini merupakan hasil dari pengukuran tingkat kapabilitas manajemen keamanan informasi, temuan setiap proses, serta saran perbaikan yang berguna untuk membantu Dinas Komunikasi dan Informatika Kabupaten Kediri mencapai tingkat kapabilitas keamanan informasi yang belum tercapai.

3. HASIL DAN PEMBAHASAN

Setelah mengumpulkan data dan memvalidasi hasil dari Diskominfo Kabupaten Kediri berdasarkan permasalahan yang ada, sehingga fokus area untuk penelitian ini adalah APO13 *Manage Security* (Mengelola Keamanan) dan DSS05 *Manage Security Services* (Mengelola

Keamanan Layanan). Berikut hasil dan pembahasan pengukuran tingkat kapabilitas manajemen keamanan informasi pada Diskominfo Kab. Kediri:

3.1 Pengukuran Tingkat Kapabilitas APO13

Berikut merupakan hasil penilaian terhadap praktik dasar dan produk kerja proses APO13 *Manage Security* yang tersaji pada tabel 2 dan tabel 3 :

Tabel 2. Pengukuran Praktik Dasar APO13

Tujuan Proses	Praktik Dasar	Skor	Skor Tujuan Proses
APO13-01 Syarat keamanan informasi dipertimbangkan dan ditangani secara efektif pada sistem.	APO13-BP1 Sistem Manajemen Keamanan Informasi (SMKI) ditetapkan dan dipelihara.	42,86% P	31,34% P
	APO13-BP3 Memantau dan meninjau SMKI.	20% P	
APO13-02 Rencana keamanan telah ditetapkan, disepakati, dan didiskusikan ke seluruh perusahaan.	APO13-BP2 Rencana penanganan risiko keamanan informasi ditetapkan dan dikelola.	33,33% P	33,33% P
APO13-03 Mengeimplementasikan solusi pada keamanan informasi dengan konsisten pada perusahaan.	APO13-BP3 Memantau dan meninjau SMKI.	20% P	20% P

Skor yang didapatkan pada tabel 2 diperoleh sebab Sistem Manajemen Keamanan Informasi (SMKI) pada Diskominfo Kab. Kediri belum diterapkan dan dikembangkan sesuai dengan ruang lingkup yang ditentukan. Selama ini, praktik mengacu Peraturan Bupati SBPE yang mengatur terkait keamanan secara global.

Tabel 3. Pengukuran Produk Kerja APO13

Praktik Dasar	Produk Kerja	Ada?	Skor
APO13-BP1 Sistem Manajemen Keamanan Informasi (SMKI) ditetapkan dan dipelihara.	APO13-WP1 Kebijakan SMKI.	Y	50% P
	APO13-WP2 Cakupan lingkup SMKI.	T	
APO13-BP2 Rencana penanganan risiko keamanan informasi ditetapkan dan dikelola.	APO13-WP3 Dokumen perencanaan solusi risiko keamanan informasi.	T	0% N
	APO13-WP4 Studi kasus risiko bisnis keamanan informasi.	T	
APO13-BP3 Memantau dan meninjau SMKI.	APO13-WP5 Laporan hasil audit SMKI.	T	0% N
	APO13-WP6 Rekomendasi peningkatan SMKI.	T	

Produk kerja harus tercapai sebagai bukti bahwa praktik dasar telah dilaksanakan. Selanjutnya skor rata-rata praktik dasar dan skor rata-rata produk kerja dihitung untuk mengetahui skor keseluruhan proses [13] pada APO13 yang disajikan berikut.

$$Outcomes = \frac{\sum(\text{Skor Tujuan Proses})}{\text{Tujuan Proses}} \quad \%$$

$$= \frac{(31{,}43 + 33{,}33 + 20)}{3} \quad \%$$

$$= 28{,}25\%$$

$$\text{Produk Kerja} = \frac{\sum(\text{Skor Produk Kerja})}{\text{Praktik dasar}} \quad \%$$

$$= \frac{(50 + 0 + 0)}{3} \quad \%$$

$$= 16{,}67\%$$

$$\text{Skor Proses} = \frac{(Outcomes + \text{Produk Kerja})}{2} \quad \%$$

$$= \frac{(28{,}25 + 16{,}67)}{2} \quad \%$$

$$= 22{,}46\%$$

Berdasarkan perhitungan skor proses diketahui proses APO13 mendapatkan skor 22,46% dan masuk dalam kategori P (*Partially Achieved*). Oleh karena itu, APO13 berada pada level 1 dan tidak dapat dilanjutkan perhitungan pada level 2 karena tidak memenuhi kategori F (*Fully Achieved*).

3.2 Pengukuran Tingkat Kapabilitas DSS05

Berikut merupakan hasil penilaian terhadap praktik dasar dan produk kerja proses DSS05 *Manage Security Services* yang disajikan pada tabel 4 dan tabel 5:

Tabel 4. Pengukuran Praktik Dasar DSS05

Tujuan Proses	Praktik Dasar	Skor	Skor Tujuan Proses
DSS05-01 Memastikan keamanan jaringan dan komunikasi memenuhi kebutuhan bisnis.	DSS05-BP1 Perlindungan dari *malware*.	100% F	82,22% L
	DSS05-BP2 Pengelolaan keamanan konektivitas serta jaringan.	66,67% L	
	DSS05-BP7 Pemantauan infrastruktur keamanan.	80% L	
DSS05-02 Melindungi informasi (proses, simpan, transmisi) pada perangkat titik akhir.	DSS05-BP1 Perlindungan dari *malware*.	100% F	100% F
	DSS05-BP3 Pengelolaan keamanan hingga titik akhir.	100% F	
DSS05-03 Selurh pengguna/staf dapat dikenali secara unik dan memiliki hak akses disesusaikan peran bisnis.	DSS05-BP4 Pengelolaan identitas pengguna dan akses logis.	62,50% L	62,50% L
DSS05-04 Langkah-langkah fisik ada untuk melindungi data terhadap akses, penghancuran, dan pemrosesan yang tidak sah saat diproses, disimpan, atau dikirim.	DSS05-BP5 Pengelolaan akses fisik terhadap aset TI.	42,86% P	42,86% P
DSS05-05 Informasi secara elektronik dipastikan aman saat proses penyimpanan, pengiriman, dan penghancuran.	DSS05-BP6 Pengelolaan dokumen sensitif dan perangkat *output.*	60% L	60% L

Berdasarkan tabel 4 diketahui bahwa Diskominfo Kab. Kediri telah menerapkan dan memelihara langkah-langkah pencegahan untuk melindungi titik akhir dan manajemen keamanan layanan telah dilakukan dengan baik namun kurang dalam hal pendokumentasian.

Tabel 5. Pengukuran Produk Kerja DSS05

Praktik Dasar	Produk Kerja	Ada?	Skor
DSS05-BP1 Perlindungan dari *malware*.	DSS05-WP1 Kebijakan terkait pencegahan *malware*.	Y	100% F
	DSS05-WP2 Evaluasi potensi ancaman.	Y	

DSS05-BP2 Pengelolaan keamanan konektivitas serta jaringan.	DSS05-WP3 Kebijakan keamanan jaringan dan konektivitas.	Y	100% F
	DSS05-WP4 Hasil *penetration test.*	Y	
DSS05-BP3 Pengelolaan keamanan hingga titik akhir.	DSS05-WP5 Peraturan tentang keamanan untuk *end-point*.	Y	100% F
DSS05-BP4 Pengelolaan identitas pengguna dan akses logis.	DSS05-WP6 Persetujuan hak akses pengguna.	T	0% N
	DSS05-WP7 Hasil ulasan akun (termasuk pengguna dan hak istimewa).	T	
DSS05-BP5 Pengelolaan akses fisik terhadap aset TI.	DSS05-WP8 Persetujuan akses.	Y	50% P
	DSS05-WP9 Akses log.	T	
DSS05-BP6 Pengelolaan dokumen sensitif dan perangkat *output.*	DSS05-WP10 Inventarisasi dokumen dan perangkat sensitif.	Y	50% P
	DSS05-WP11 Hak Akses Istimewa.	T	
DSS05-BP7 Pemantauan infrastruktur keamanan.	DSS05-WP12 Log peristiwa keamanan	Y	100% F
	DSS05-WP13 Karaktersitik insiden keamanan.	Y	
	DSS05-WP14 Tiket insiden keamanan.	Y	

Produk kerja harus tercapai sebagai bukti bahwa praktik dasar telah dilaksanakan. Selanjutnya skor rata-rata praktik dasar dan skor rata-rata produk kerja dihitung untuk mengetahui skor keseluruhan proses [13] pada DSS05 yang disajikan berikut.

$$Outcomes = \frac{\sum(\text{Skor Tujuan Proses})}{\text{Tujuan Proses}} \quad \%$$

$$= \frac{(82{,}22 + 100 + 62{,}5 + 42{,}86 + 60)}{5} \%$$

$$= 69{,}52\%$$

$$\text{Produk Kerja} = \frac{\sum(\text{Skor Produk Kerja})}{\text{Praktik dasar}} \%$$

$$= \frac{(100+100+100+0+50+50+100)}{7} \%$$

$$= 71{,}43\%$$

$$\text{Skor Proses} = \frac{(Outcomes + \text{Produk Kerja})}{2} \%$$

$$= \frac{(69{,}52 + 71{,}43)}{2} \%$$

$$= 70{,}47\%$$

Berdasarkan perhitungan skor proses diketahui proses DSS05 mendapatkan skor 70,47% dan masuk dalam kategori L (*Largely Achieved*). Oleh karena itu, DSS05 berada pada level 1 dan tidak dapat dilanjutkan perhitungan pada level 2 karena tidak memenuhi kategori F (*Fully Achieved*).

3.3 Hasil Temuan dan Rekomendasi

Berdasarkan perhitungan tingkat kapabilitas manajemen keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri yang disajikan pada tabel 6, proses APO13 mendapatkan skor 22,46% pada kategori P *(Partially Achieved)* sedangkan DSS05 mendapatkan skor yang lebih tinggi yaitu 70,47% pada kategori L *(Largely Achieved)*. Dengan demikian, kedua proses pada level yang sama yaitu level 1 *(Performed)* yang menandakan pada level ini proses yang diimplementasikan mendekati atau mencapai tujuan prosesnya.

Tabel 6. Hasil Pengukuran Tingkat Kapabilitas

	0	1	2		3		4		5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
APO13	100% F	22,46% P								
DSS05	100% F	70,47% L								

Rekomendasi berdasarkan hasil dan temuan pada APO13 adalah Membangun dan mengembangkan SMKI mengacu Peraturan BSSN No 4 Tahun 2021 dan Permenkominfo nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang kemudian diadopsi menjadi Peraturan Bupati Kediri serta mengkomunikasikan SMKI secara berkala kepada seluruh staf sehingga SMKI dapat lebih baik dan berkelanjutan; Memformulasikan dan mengembangkan pemetaan perencanaan; Menangani risiko keamanan informasi sesuai dengan tujuan strategis dan arsitektur perusahaan serta menggabungkan solusi keamanan informasi yang tepat dan optimal dengan sumber daya terkait, tanggung jawab dan prioritas dalam pengelolaan risiko keamanan informasi yang teridentifikasi; Melakukan tinjauan berkala terhadap kinerja SMKI, termasuk kepatuhan terhadap prinsip dan tujuan SMKI, serta audit keamanan dan hasil insiden, hasil pengukuran kinerja, dan umpan balik pemangku kepentingan untuk peningkatan penerapan SMKI.

Sedangkan rekomendasi berdasarkan hasil dan temuan DSS05 adalah: Membuat daftar izin perangkat-perangkat untuk memiliki akses pada informasi perusahaan dan jaringan Diskominfo Kab. Kediri dengan mengkonfigurasi perangkat agar memaksa staf masuk menggunakan *password*; Rutin melaksanakan *penetration test* untuk menentukan kelayakan dari proteksi jaringan; Kelola semua perubahan hak akses (pembuatan, modifikasi, penghapusan) sehingga diimplementasikan secara tepat waktu, hanya berdasarkan peristiwa yang disetujui dan didokumentasikan yang disetujui oleh manajemen. Catat semua peristiwa terkait keamanan data yang dilaporkan oleh perangkat pemantauan data dan konfigurasikan ruang lingkup penyimpanan data berdasarkan pertimbangan risiko. Data ini harus disimpan untuk jangka waktu tertentu agar dapat digunakan untuk penelitian selanjutnya.

4. KESIMPULAN DAN SARAN

Berdasarkan perhitungan tingkat kapabilitas manajemen keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri, proses APO13 mendapatkan skor 22,46% pada kategori P *(Partially Achieved)* sedangkan DSS05 mendapatkan skor yang lebih tinggi yaitu 70,47% pada kategori L *(Largely Achieved)*. Dengan demikian, kedua proses pada level yang sama yaitu level 1 *(Performed)* yang menandakan pada level ini proses yang diimplementasikan mendekati atau mencapai tujuan prosesnya.

Adapun saran yang dapat diusulkan bagi Dinas Komunikasi dan Informatika Kabupaten Kediri disarankan untuk mempertimbangkan dan melaksanakan saran perbaikan pada proses APO13 *Manage Security* dan DSS05 *Manage Security Services* serta secara rutin mengkomunikasikan praktik kerja sehingga staf teknis maupun pihak manajemen memahami kebutuhan atau masalah di lapangan. Sedangkan bagi penelitian selanjutnya disarankan untuk menggunakan fokus proses berbeda dengan pemetaan tujuan perusahaan dan tujuan TI berbeda sehingga didapatkan hasil evaluasi keamanan informasi yang beragam.

5. DAFTAR RUJUKAN

[1] Rosmiati and I. Riadi, "Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001 : 2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ)," *Semin. Nas. Teknol. Inf. Dan Multimed. 2016*, vol. 4, no. 1, pp. 1–2, 2016.

[2] R. Sarno and I. Iffano, *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press, 2009.

[3] M. Hassanzadeh, N. Jahangiri, and B. Brewster, *A Conceptual Framework for Information Security Awareness, Assessment, and Training*. Elsevier Inc., 2013. doi: 10.1016/B978-0-12-411474-6.00006-2.

[4] M. Lenawati, W. W. Winarno, and A. Amborowati, "Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5," *Sentra Penelit. Eng. dan Edukasi*, vol. 9, no. 1, pp. 44–49, 2017, [Online]. Available: http://speed.web.id/jurnal/index.php/speed/article/view/220

[5] R. Sheikhpour and N. Modiri, "An approach to map COBIT processes to ISO/IEC 27001 information security management controls," *Int. J. Secur. its Appl.*, vol. 6, no. 2, pp. 13–28, 2012.

[6] ITGID, "Pentingnya Implementasi COBIT bagi IT Perusahaan," 2016. https://itgid.org/cobit-5-adalah/ (accessed Oct. 28, 2022).

[7] ISACA, *Enabling Processes*. ISACA, 2012. [Online]. Available: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT5-Ver2-enabling.pdf.

[8] J. Wulandari, "EVALUASI KEAMANAN INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI DENGAN MENGGUNAKAN INDEKS KAMI," Brawijaya University, 2017.

[9] A. Wulansari, C. L. Prasetyo, S. Mukaromah, D. S. Y. Kartika, E. M. Safitri, and A. R. E. Najaf, "E-Government Risk Optimization Capability Measurement," vol. 04012, pp. 1–5, 2022.

[10] P. S. K. Shesa, S. Mukaromah, and D. Ridwandono, "COBIT 4.1: PERANCANGAN PERANGKAT PENGUKURAN TINGKAT KEMATANGAN PERENCANAAN DAN PENGELOLAAN TEKNOLOGI INFORMASI.," *J. Inform. dan Sist. Inf.*, vol. 02, no. 2, pp. 432–438, 2021.

[11] M. N. Fuad and I. Riadi, "Risk Management Assessment on Human Resource Information Technology Services using COBIT 5," *Int. J. Comput. Appl.*, vol. 175, no. 23, pp. 12–19, 2020, doi: 10.5120/ijca2020920756.

[12] ISACA, *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5*. 2013.

[13] S. Mukaromah *et al.*, "Alignment of Business Goals With IT Goals By Measuring The Level of Capability Using Cobit 5," pp. 354–358, 2022, doi: 10.1109/itis57155.2022.10010265.