Evaluasi Kapabilitas Layanan Keamanan Teknologi Informasi Menggunakan COBIT 5 *Process Assessment Model* (DSS05)

Muhammad Fariz Arizali Effendi[1], Andi Reza Perdanakusuma[2], Widhy Hayuhardhika Nugraha Putra[3]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya

Email: aemfariz@student.ub.ac.id[1], andireza@ub.ac.id[2], widhy@ub.ac.id[3]

Abstrak

DISKOMINFO Kota Malang merupakan instansi penyelenggara keperluan berkaitan dengan pemanfaatan teknologi informasi. Aktivitas pengelolaan keamanan TI di DISKOMINFO Kota Malang dilakukan oleh Bidang APTIKA. Pemanfaatan fungsi TI didasari dengan prinsip kerahasiaan, integritas, dan ketersediaan. Seiring kemajuan teknologi, dibutuhkan kewaspadaan dalam pengelolaan keamanan TI agar kegiatan operasional berjalan dengan baik, mencegah ancaman potensial keamanan, dan meningkatkan efisiensi kinerja. Karena alasan tersebut, perlu dilakukan pengukuran kualitas pengelolaan keamanan TI untuk memastikan teknologi informasi yang diterapkan aman dan sesuai strategi instansi. Pengukuran kapabilitas keamanan TI di DISKOMINFO Kota Malang dilakukan dengan membandingkan kondisi pengelolaan keamanan TI yang telah dicapai dengan kondisi yang diinginkan. Penelitian ini menggunakan metode kualitatif berdasarkan panduan COBIT 5 berfokus pada proses DSS05 (Manage Security Services). Pengumpulan data dilakukan dengan observasi, penggunaan instrumen lembar penilaian COBIT 5, lembar checklist, dan wawancara langsung. Berdasarkan hasil penelitian, hasil proses DSS05 (Manage Security Services) mencapai level 0 (Incomplete Process). DISKOMINFO Kota Malang mengharapkan proses DSS05 (Manage Security Services) dapat mencapai level 2 (Managed Process). Sehingga didapatkan kesenjangan sebesar dua level. Kemudian, didapati sebanyak 15 rekomendasi dan roadmap perbaikan kepada DISKOMINFO Kota Malang untuk mencapai target level yang diinginkan.

Kata kunci: Evaluasi, Keamanan, COBIT 5, Kapabilitas, DSS05

Abstract

Dinas Komunikasi dan Informatika (DISKOMINFO) is a government agency which provides IT services to local government (in this case Malang City Government). The activities of managing IT security in DISKOMINFO Malang City are conducted by the Application and Information Sector. Utilization of IT functions is based on the principles of confidentiality, integrity and availability. As technology advances it takes vigilance in the management of IT security to make agency operations run properly, preventing potential security threats, and can improve performance efficiency. For this reason, it is necessary to measure the quality of IT security management to ensure that the information technology implemented is safe and in accordance with agency strategies. Measurement of IT security capabilities at DISKOMINFO Malang City is done by comparing the conditions of IT security management that have been achieved with the conditions desired by the agency. This study uses a qualitative method based on COBIT 5 guidelines focusing on the DSS05 (Manage Security) process. Data collection is done by observation, use of COBIT 5 assessment sheet instruments, checklist sheets, and direct interviews. Based on the research results, the results obtained in the DSS05 (Manage Security Services) process reached level 0 (Incomplete Process). DISKOMINFO Malang City hopes that DSS05 (Manage Security Services) processes can reach level 2 (Managed Process). So that there is a gap of two level in the DSS05 process. Then, there were 15 recommendations and improvement roadmaps are presented to DISKOMINFO Malang City to reach the desired target level.

Keywords: *Evaluation, Security, COBIT 5, Capability Level, DSS05*

A. PENDAHULUAN

Tata kelola keamanan teknologi informasi merupakan kebutuhan primer bagi setiap instansi publik maupun non-publik dalam Revolusi Industri 4.0. Revolusi Industri 4.0 hadir dalam kehidupan masyarakat dengan membawa tren otomasi dan *internet of things*. Era dimana pemanfaatan teknologi, *big data*, dan *cloud computing* mendukung penerapan otomasi dan membangun hubungan untuk bertukar informasi melalui jaringan. Ancaman dan gangguan keamanan *cyber* adalah tanggung jawab bersama setiap instansi publik. Instansi perlu

membangun komitmen dan budaya kesadaran keamanan informasi mulai dari tingkatan *top level management* sampai dengan pegawai teknis. Seluruh pihak dalam instansi harus berkontribusi secara optimal dan proporsional sesuai dengan perannya masing-masing. Keamanan informasi yang baik hanya dapat dicapai melalui penerapan sejumlah upaya-upaya teknis yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai (Suharyanto, 2019).

Berdasarkan data dari *Security Report, Check Point* (2018), terdapat sebanyak 64% Lembaga Publik di seluruh dunia bermasalah dengan keamanan teknologi informasi. Salah satu penyebabnya adalah belum optimalnya penerapan tata kelola keamanan teknologi informasi. Hal ini perlu disikapi serius oleh instansi publik untuk meningkatkan perbaikan di aspek tata kelola keamanan teknologi informasi. Solusi teknis memang dapat memecahkan permasalahan, namun tanpa adanya perbaikan tata kelola akan menjadi sia-sia.

Dinas Komunikasi dan Informatika Kota Malang merupakan instansi publik yang berfungsi melayani masyarakat secara profesional dalam bidang informasi dan komunikasi. Dinas Komunikasi dan Informatika Kota Malang selalu menerapkan mekanisme tata kelola keamanan teknologi informasi melalui kebijakan instansi untuk efisiensi operasional dan anggaran, optimalisasi risiko keamanan teknologi informasi, penanganan teknis dari berbagai macam kemungkinan terjadinya serangan eksternal, pembatasan hak akses dalam lingkup internal instansi, kebijakan pengaturan *firewall*, dan penggunaan sistem operasi *open source*.

COBIT 5 dipilih untuk menangani permasalahan tata kelola keamanan teknologi informasi karena menyajikan kerangka kerja yang komprehensif dalam membantu instansi mencapai tujuan berkaitan dengan pengelolaan keamanan informasi dan aset teknologi. COBIT 5 bersifat generik dan

bermanfaat untuk instansi dari semua ukuran, baik komersial ataupun sektor publik (ISACA, 2012).

DISKOMINFO Kota Malang

Dinas Komunikasi dan Informatika Kota Malang adalah instansi di bawah pemerintah Kota Malang yang bertujuan melayani masyarakat secara profesional dalam bidang teknologi informasi dan komunikasi yang selalu meningkatkan keprofesionalitasan agar visi, misi, tujuan, dan rencana strategis yang dicanangkan organisasi dapat dicapai.

RACI Chart

RACI *Chart* merupakan pemberian tugas dan wewenang pada masing-masing tingkat kewajiban yang diusulkan untuk praktik proses pada peran struktur yang berbeda. RACI Chart seringkali digunakan sebagai metode untuk memilih responden yang akan menjadi penyedia informasi yang berguna dalam aktivitas penilaian sebuah proses. Terdapat 4 tingkatan pada RACI *Chart*, yaitu *Responsible* (R), *Accountable* (A), *Consulted* (C), dan *Informed* (I). (PMBOK, 2013).

COBIT 5

COBIT 5 adalah pedoman dari ISACA yang membahas mengenai tata kelola teknologi informasi. COBIT 5 memberikan kerangka kerja yang menyeluruh yang dapat mendukung dalam mencapai tujuan instansi, baik untuk bidang tata kelola maupun keamanan teknologi informasi. Dalam COBIT 5, terdapat suatu model yang disebut Process Assessment Model (PAM) yang digunakan untuk menilai kapabilitas suatu proses berdasarkan pada satu atau lebih model referensi proses. Model ini adalah

dasar untuk melakukan penilaian mengenai kemampuan dalam pengelolaan TI. Proses penilaian diuji dengan memungkinkan proses penilaian yang dapat dipercaya, konsisten, dan dapat diulang di bidang tata kelola dan manajemen teknologi informasi (ISACA, 2012).

Capability Level

C*apability level* dinyatakan dari 0 hingga 5. *Capability level* 0 tidak memiliki atribut. Level 0 menunjukkan proses yang tidak diimplementasikan atau proses yang tidak berhasil untuk setidaknya mencapai sebagian hasilnya. Berdasarkan *Self-Assessment Guide: Using* COBIT 5 – ISACA (2013), *capability level* terdiri dari 6 level, antara lain:

1. Level 0 – *Incomplete*

   Pada level ini, proses ini tidak memiliki kemampuan dasar dan mencerminkan pendekatan yang tidak lengkap untuk menangani tujuan tata kelola dan manajemen. Selain itu, proses tidak memiliki tujuan untuk dicapai. Karena alas an ini, level ini tidak memiliki atribut.

2. Level 1 – *Performed*

   Level ini menunjukkan bahwa proses yang diimplementasikan mencapai tujuan prosesnya. Prosesnya sudah ada dan mencapai tujuannya sendiri

3. Level 2 – *Managed*

   Level ini menunjukkan bahwa proses yang dilakukan sekarang diimplementasikan dengan terencana, dipantau, dan diselaraskan dan hasilnya telah ditetapkan, dikontrol, dan dipelihara dengan tepat. Proses ini mencapai tujuannya melalui penerapan serangkaian aktivitas dasar, namun lengkap.

4. Level 3 – *Established*

   Level ini menunjukkan bahwa proses yang diatur saat ini diterapkan menggunakan proses yang ditetapkan dan dapat mencapai hasil dari proses tersebut.

5. Level 4 – *Predictable*

   Level ini mengimplementasikan proses dalam batas yang ditetapkan yang memungkinkan pencapaian hasil prosesnya.

6. Level 5 – *Optimizing*

   Level ini mengimplementasikan proses dengan cara yang memungkinkan untuk mencapai tujuan bisnis yang relevan, saat ini, dan yang diproyeksikan.

Rating Scale

Setiap atribut yang ada pada masing-masing level dinilai menggunakan skala peringkat (*rating scale*) yang didefinisikan dalam standar ISO/IEC 15504. Peringkat (*rating*) ini terdiri dari :

1. N – *Not Achieved*. Terdapat sedikit atau tidak ada bukti capaian atribut yang didefinisikan dalam proses yang dinilai. Peringkat ini memiliki pencapaian 0 – 15%
2. P – *Partially Achieved*. Terdapat beberapa bukti pendekatan dan capaian dari atribut yang ditentukan dalam proses yang dinilai. Beberapa bagian capaian atribut mungkin tidak dapat diperkirakan. Peringkat ini memiliki pencapaian lebih dari 15% - 50%.
3. L – *Largely Achieved*. Terdapat bukti pendekatan sistematis dan capaian yang substansial dari atribut yang ditentukan dalam proses yang dinilai. Beberapa kekurangan yang berhubungan dengan atribut

ini mungkin ada dalam proses yang dinilai. Peringkat ini memiliki pencapaian lebih dari 50% – 85%.

4. F – *Fully Achieved*. Terdapat bukti pendekatan yang komprehensif dan sistematis dan pencapaian lengkap dari atribut yang ditentukan dalam proses yang dinilai. Tidak ada kekurangan yang berarti yang berhubungan dengan atribut ini ada dalam proses yang dinilai. Peringkat ini memiliki pencapaian lebih dari 85% - 100%.

Proses DSS05 (*Manage Security Services*)

Proses DSS05 (*Manage Security Services*) bertujuan melakukan perlindungan informasi organisasi untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh organisasi sesuai dengan kebijakan keamanan. Membangun dan memelihara peran keamanan informasi dan hak akses serta melakukan monitoring keamanan. Proses ini bertujuan memperkecil dampak bisnis dari kerentanan keamanan informasi operasional dan insiden terkait (ISACA, 2012)

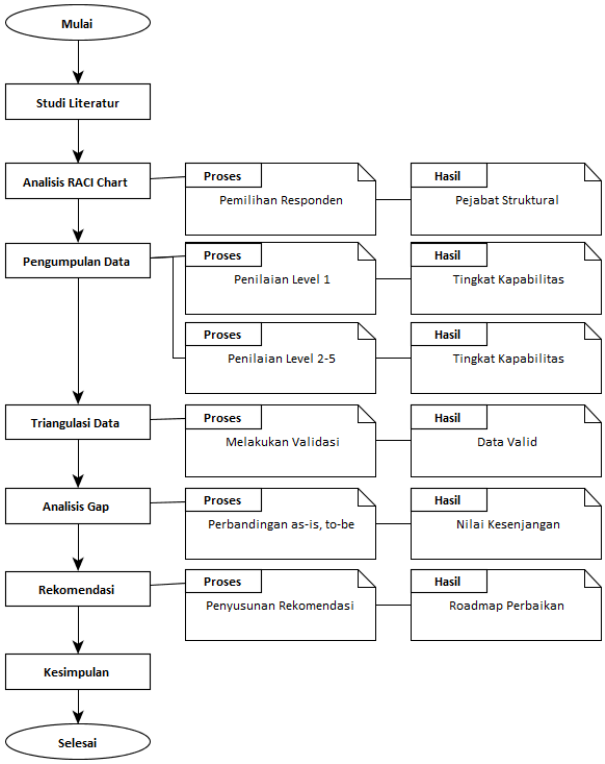
Roadmap Pelaksanaan

Roadmap adalah proses penyusunan program dan perencanaan penelitian sedemikian rupa sehingga mampu memperkirakan kebutuhan teknologi ke depan dalam kurun waktu tertentu melalui identifikasi, analisis, dan sintetis hasil penelitian yang ada (Gunawan & Pratama, 2018).

B. METODE

Metodologi Penelitian yang digunakan pada penelitian ini merujuk pada panduan penelitian dengan metodologi kualitatif pada *Scientific*

Research in Information Systems oleh Jan Recker (2013) dan *Self Assesment* pada COBIT 5. Alur tahapan pengerjaan penelitian dijelaskan pada Gambar 1.



Gambar 1. Alur Penelitian

Studi Literatur

Tahapan awal dari penelitian adalah studi literatur. Studi literatur diperlukan untuk mencari dan mempelajari literatur yang berhubungan dengan obyek yang sedang diteliti untuk menunjang pengerjaan penelitian. Literatur yang digunakan diperoleh dari sumber-sumber seperti buku, jurnal ilmiah, dan website yang mendukung topik yang diteliti. Dengan adanya studi literatur diharapkan dapat membantu peneliti dalam pengerjaan tahap-tahap penelitian setelahnya.

RACI Chart

Analisis RACI *Chart* digunakan untuk memetakan peran pemangku kepentingan di DISKOMINFO Kota Malang yang berkaitan dengan pengelolaan keamanan teknologi informasi. Untuk melakukan pemetaan tersebut, peneliti melakukan wawancara pada narasumber yang memiliki pengetahuan luas mengenai kinerja pengelolaan keamanan teknologi informasi. Cobit 5 sudah memberikan pedoman terkait peran masing-masing pemangku kepentingan pada tiap proses tata kelola, penelitian ini bermaksud untuk mengkategorikan peran para pemangku kepentingan pada DISKOMINFO sesuai dengan prinsip Cobit 5.

Pengumpulan Data

Data utama yang dibutuhkan dalam penelitian ini adalah data terkait *self-assessment* yang dilakukan dengan pengisian lembar *checklist* terkait penilaian kapabilitas di DISKOMINFO Kota Malang yang diadaptasi dari dokumen COBIT 5 *Proces Assessment Model* dan wawancara pada narasumber, kemudian terkait data bukti *work product* didapatkan melalui studi dokumen maupun observasi.

Triangulasi Data

Proses Triangulasi yang digunakan adalah triangulasi metode. Triangulasi bertujuan untuk memvalidasi data penelitian dengan membandingkan dan menganalisis hasil yang didapat dari wawancara yang diadaptasi dari model kapabilitas COBIT 5 dengan observasi bukti pengelolaan yang dikenal dengan istilah *work product*. (Bogdan & Biklen, 2006).

Analisis Gap

Analisis gap bertujuan untuk memberikan informasi mengenai kesenjangan antara tingkat kapabilitas tata kelola proses DSS05 saat ini dan tingkat kapabilitas DSS05 di masa depan yang diharapkan oleh DISKOMINFO Kota Malang. Informasi kesenjangan tingkat kapabilitas ini menjadi dasar untuk membuat roadmap untuk mengejar level harapan tata kelola DSS05 di masa depan.

Roadmap Tata Kelola TI

Luaran rekomendasi dari penelitian berupa roadmap praktik tata kelola yang perlu dilakukan DISKOMINFO kota Malang dimasa depan. Untuk mengembangkan rekomendasi, maka diperlukan masukan berupa informasi terkait *work product* tata kelola TI yang belum dilakukan organisasi untuk kemudian diprioritaskan untuk dijalankan selama periode tertentu menggunakan analisis dampak & kepentingan. Kemudian hasil luaran dari analisis dampak & kepentingan di lakukan triangulasi oleh *expert judgment* yang sudah berpengalaman pada bidang tata kelola TI agar hasil roadmap menjadi valid.

C. HASIL DAN PEMBAHASAN

Analisis RACI Chart

Berdasarkan hasil pemetaan peran pada RACI *Chart* dengan peran / jabatan dalam organisasi pada Tabel 1, diperoleh bahwa penerapan pengelolaan layanan keamanan proses DSS05 di DISKOMINFO Kota Malang dilakukan oleh Kepala Seksi Pemberdayaan TIK, Pengelola Jaringan dan Infrastruktur, dan Kepala Seksi Pengelolaan e-Gov.

Tabel 1. Analisis RACI *Chart* Proses

Komponen	Peran	Jabatan Organisasi
R	*Head IT Administration*	Kepala Seksi Pemberdayaan TIK
R	*Information Security Manager*	Pengelola Jaringan dan Infrastruktur
A	*Chief Information Security Officer*	Kepala Seksi Pengelolaan e-Gov

Hasil Temuan Observasi

Berdasarkan lembar *checklist* dan observasi dokumen pada proses DSS05 yang berupa *Base Practices* dan *Work Product*. Pada proses DSS05 terdapat tujuh *Base Practices* (BP) yang digunakan untuk mengukur penilaian. Tabel 2 menjelaskan mengenai *base practices* pada proses DSS05 (*Manage Security Services*) beserta dokumen pendukungnya.

Tabel 2. Pemetaan Dokumen *Base Practices*

Base Practices	Keterangan	Dokumen
DSS05-BP1	Menerapkan dan memelihara langkah-langkah pencegahan, detektif, dan korektif	Buku Standar Tata Kelola Keamanan Data dan Informasi (SOP Pemasangan Perangkat Lunak)
DSS05-BP2	Menggunakan langkah-langkah keamanan dan prosedur terkait untuk melindungi informasi dari semua metode konektivitas	Belum Ada
DSS05-BP3	Memastikan *endpoint* (laptop, desktop, server, dan perangkat lunak seluler lainnya) diamankan pada tingkat yang sama dengan atau lebih besar dari persyaratan keamanan yang ditetapkan	Belum Ada
DSS05-BP4	Memastikan bahwa semua pengguna memiliki hak akses informasi sesuai dengan persyaratan bisnis mereka	Peraturan Walikota nomor 46 tahun 2012 dan Standar Kontrol Akses Logik
DSS05-BP5	Menetapkan dan menerapkan prosedur untuk memberikan, membatasi, dan mencabut akses	SOP Permintaan hak akses dan Standar Pemeliharaan Perangkat Lunak
DSS05-BP6	Menetapkan pengamanan fisik, praktik	Belum Ada

	akuntansi, dan manajemen inventaris yang tepat atas aset TI	
DSS05-BP7	Dengan menggunakan alat deteksi intrusi, pantau infrastruktur untuk akses yang tidak sah, dan pastikan semua kejadian terintegrasi dengan pemantauan kejadian umum dan manajemen insiden	Belum Ada

Dari ketujuh *Base Practices* yang telah disebutkan diatas, masing-masing BP tersebut diturunkan menjadi beberapa *Work Product* (WP) yang digunakan untuk melakukan penilaian proses DSS05. Tabel 3 menjelaskan mengenai pemetaan dokumen *Work Products* DSS05.

Tabel 3. Pemetaan Dokumen *Work Products* DSS05

Work Products	**Keterangan**	**Dokumen**
APO09-WP6	Konten persetujuan tingkat layanan	Belum Ada
APO01-WP14	Konten klasifikasi data	Belum Ada
APO03-WP6	Konten model arsitektur informasi	Belum Ada
APO09-WP7	Konten perjanjian tingkat operasional (OLA) yang mendukung perjanjian tingkat layanan	Belum Ada
BAI09-WP2	Konten pemeriksaan inventori fisik	Belum Ada
DSS06-WP10	Konten hasil dari transaksi	Belum Ada
APO01-WP8	Konten hubungan peran dan tanggung jawab TI	Peraturan Walikota nomor 46 tahun 2012
APO03-WP6	Konten model arsitektur informasi	Belum Ada
DSS05-WP1	Konten pencegahan perangkat lunak berbahaya	SOP Pemasangan Perangkat Lunak
DSS05-WP2	Konten evaluasi dari ancaman potensial keamanan	Belum Ada
DSS05-WP3	Konten kebijakan keamanan pada konektivitas	Belum Ada
DSS05-WP4	Konten hasil pengujian keamanan	Belum Ada
DSS05-WP5	Konten kebijakan keamanan pada perangkat *endpoint* (laptop, computer, server, dan perangkat lainnya)	Standar Penggunaan Sumber Daya Teknologi Informasi
DSS05-WP6	Konten persetujuan hak akses pengguna	Standar Kontrol Akses Logik
DSS05-WP7	Konten hasil peninjauan ulang (*review*) pengguna dan hak aksesnya	Belum Ada

DSS05-WP8	Konten persetujuan permintaan hak akses	SOP Permintaan hak akses
DSS05-WP9	Konten *access logs* pada sistem	Standar Pemeliharaan Perangkat Lunak untuk Server
DSS05-WP10	Konten tentang karakteristik risiko keamanan	Belum Ada
DSS05-WP11	Konten daftar peristiwa keamanan informasi	Belum Ada
DSS05-WP12	Konten tiket insiden keamanan	Belum Ada
DSS05-WP13	Konten inventarisasi dokumen dan perangkat penting	Belum Ada
DSS05-WP14	Konten wewenang hak akses	Standar Kontrol Akses Logik

Persentase tingkat kapabilitas diukur dari pencapaian atribut proses. Pada Proses DSS05, penilaian atribut proses 1.1 didapatkan persentase sebesar 32% dengan kategori *Partially Achieved*. Sehingga tidak dapat dilakukan penilaian pada atribut proses 2.1 dan selanjutnya. Tabel 4 menjelaskan pencapaian tingkat kapabilitas DSS05.

Tabel 4. Pencapaian Tingkat Kapabilitas

NO	Tingkat Kapabilitas	Target	Capaian	Persentase
1	PA 1.1	22	7	32%
2	PA 2.1	10	0	0%
	PA 2.2	5	0	0%

Hasil penilaian tingkat kapabilitas proses DSS05 *Manage Security Services* pada DISKOMINFO Kota Malang dijelaskan pada Tabel 12.

Tabel 5. Penilaian Tingkat Kapabilitas

DSS05	L0	L1	L2	L3	L4	L5
Rate		P	-	-	-	-
CP	v					
%		32%	-	-	-	-

Setelah dilakukan penilaian proses DSS05, maka dilakuan triangulasi metode. Tahap triangulasi metode dilakukan pemeriksaan

keabsahan data dari Teknik observasi, wawancara, dan hasil lembar penilaian. Tabel 6 menjelaskan hasil triangulasi pada proses DSS05.

Tabel 6. Triangulasi Proses DSS05

	Hasil	Observasi dan Wawancara	Validasi
DSS05	R1:0	Sesuai	V
	R2:0	Sesuai	V
	R3:0	Sesuai	V

Setelah dilakukan triangulasi untuk memeriksa keabsahan data, langkah selanjutnya adalah Analisis *Gap*. DISKOMINFO mengharapkan tata kelola keamanan teknologi informasi berada di level dua atau paling tidak dapat disebut terkelola.. Tabel 7 menjelaskan kesenjangan level proses DSS05.

Tabel 7. Analisis Kesenjangan DSS05

Nama Proses	Level saat ini	Level target	Kesenjangan
DSS05 (*Manage Security Services*)	0	2	2

Pembahasan

Tingkat kapabilitas yang dicapai oleh Dinas Komunikasi dan Informatika Kota Malang pada proses DSS05 berada pada level 0 yaitu *Incomplete Process* yang berarti Dinas Komunikasi dan Informatika Kota Malang belum berhasil mengimplementasikan proses, proses DSS05 hanya mencapai skala *rating Partially Achieved* pada PA 1.1 yang berarti *evidence* belum memenuhi keseluruhan indikator setiap atribut yang telah ditetapkan pada buku panduan COBIT.

Setelah dilakukan pengukuran tingkat kapabilitas proses DSS05, dilakukan analisis gap untuk membandingkan kondisi saat ini (*as is*) dan kondisi yang diharapkan oleh instansi (*to be*). Pada proses DSS05,

didapatkan kondisi saat ini setelah dilakukan evaluasi berada pada level 0 (*Incomplete Process*), sementara kondisi yang diharapkan oleh pihak Dinas Komunikasi dan Informatika Kota Malang setidaknya dapat berada di level 2 (*Managed Process*). Sehingga didapatkan gap sebesar dua tingkat.

Pada proses DSS05 terdapat 15 rekomendasi perbaikan yang diberikan, yaitu:

1. Melengkapi dokumen yang membahas perlindungan dari ancaman *virus* dan *malware*. Dokumen harus menyertakan mengenai evaluasi dari ancaman potensial keamanan. (ID01)
2. Membuat dokumen yang membahas pengelolaan jaringan dan konektivitas. Dokumen harus menyertakan mengenai klasifikasi data, hasil pengujian keamanan, dan kebijakan keamanan pada konektivitas. (ID02)
3. Melengkapi dokumen yang menyatakan pengelolaan keamanan pada titik akhir. Dokumen harus menyertakan perjanjian yang mendukung perjanjian tingkat layanan (OLA). (ID03)
4. Melengkapi dokumen yang menyatakan pengelolaan identitas pengguna dan hak aksesnya. Dokumen harus menyertakan hasil peninjauan ulang (*review*) pengguna dan hak aksesnya. (ID04)
5. Melengkapi dokumen yang membahas pengelolaan dokumen penting dan perangkat keluaran (output) lainnya. DOkumen harus menyertakan model arsitektur informasi dan kebijakan keamanan pada perangkat *endpoint* seperti komputer, laptop, *server*, dan perangkat lainnya. (ID05)
6. Membuat dokumen yang bertujuan memenatau infrastruktur untuk setiap kegiatan yang berhubungan dengan keamanan. Dokumen harus

disertai karakteristik risiko keamanan, daftar peristiwa keamanan informasi, dan tiket risiko keamanan informasi. (ID06)

7. Melakukan identifikasi tujuan performa dari proses pengelolaan keamanan teknologi informasi. (ID07)
8. Merencanakan dan mengawasi performa proses pengelolaan kemananan teknologi informasi untuk memenuhi tujuan yang telah ditentukan. (ID08)
9. Melakukan pendefinisian tanggung jawab dan otoritas dalam melakukan proses pengelolaan keamanan teknologi informasi. (ID09)
10. Melakukan identifikasi dan menyediakan sumber daya untuk melakukan proses pengelolaan keamanan teknologi informasi. (ID10)
11. Mengelola antarmuka antara pihak yang terlibat dalam pengelolaan keamanan teknologi informasi. (ID11)
12. Menetapkan kebutuhan untuk hasil kerja proses pengelolaan keamanan teknologi informasi. (ID12)
13. Menetapkan kebutuhan dari dokumentasi dan kontrol hasil kerja. (ID13)
14. Mengidentifikasi dokumentasi dan control hasil kerja. (ID14)
15. Meninjau ulang dan menyesuaikan hasil kerja untuk memenuhi kebutuhan yang telah didefinisikan. (ID15)

Pada masing-masing rekomendasi terdapat ID yang digunakan untuk memudahkan dalam pembuatan roadmap perbaikan proses DSS05. Tabel 16 menjelaskan roadmap perbaikan proses DSS05 *Manage Security Services*.

Tabel 8. Pelaksanaan Roadmap Perbaikan

No	ID Rekomendasi	Waktu Pelaksanaan					
		2020		2021		2022	
		Semester I	Semester II	Semester I	Semester II	Semester I	Semester II
1	ID01						
2	ID02						
3	ID03						
4	ID04						
5	ID05						
6	ID06						
7	ID07						
8	ID08						
9	ID09						
10	ID10						
11	ID11						
12	ID12						
13	ID13						
14	ID14						
15	ID15						

D. PENUTUP

Simpulan dan Saran

Berdasarkan hasil evaluasi kapabilitas pengelolaan layanan keamanan teknologi informasi di Dinas Komunikasi dan Informatika Kota Malang dengan menggunakan COBIT 5, didapatkan kesimpulan sebagai berikut.

1. Hasil observasi dan wawancara, proses DSS05 berada pada level 0 (*Incomplete Process*) dengan rincian proses atribut 1.1 mencapai kriteria *Partially Achieved*.
2. Pihak DISKOMINFO Kota Malang menginginkan proses DSS05 dapat mencapai paling tidak level 2 (*Managed Process*). Sedangkan dari hasil evaluasi proses DSS05 berada pada level 0 (*Incomplete*

Process). Hal ini menunjukkan kesenjangan sebesar dua level.

3. Terdapat 15 butir rekomendasi pada proses DSS05 yang perlu dilakukan mulai tahun 2020 dan berakhir pada tahun 2022

Berdasarkan hasil penelitian evaluasi kapabilitas layanan keamanan TI dengan menggunakan *framework* COBIT 5, maka saran yang diberikan adalah sebagai berikut.

1. Perlu untuk dilakukan eksplorasi pada proses-proses tata kelola yang masih berhubungan dengan proses DSS05 (*Manage Security Services*) yang berdasarkan *process assessment model* Cobit 5 yaitu proses EDM03 (*Ensure Risk Optimization*), dan proses APO12 (*Manage Risk*).
2. Mengembangkan penelitian ini menggunakan kerangka kerja yang masih berkaitan dengan keamanan informasi seperti ISO/IEC 27001, ISO/IEC 27002, ITIL (*Information Technology Infrastructure Library*) for *Information Security* v3, ISO 31000, dan kerangka kerja lainny

DAFTAR PUSTAKA

Bogdan, R. C. & Biklen, S. K. (2006). *Qualitative research in education: An introduction to theory and methods. Allyn & Bacon. ISBN 978-0-205-51225-6.*

Dinas Komunikasi dan Informatika Kota Malang. (2018). *Rencana Strategis 2019-2013.*

Gunawan, B. & Pratama, F. A., 2018. *Perancangan Tata Kelola Teknologi Informasi.* Yogyakarta: Andi.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*.s.l.:ISACA.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows: ISACA.

ISACA. (2012). *COBIT 5: Enabling Process.* Rolling Meadows: ISACA.

ISACA. (2013). *Assesor Guide: Using COBIT 5.* Rolling Meadows: ISACA.

ISACA. (2013). *Process Assessment Model (PAM): Using COBIT 5.* Rolling Meadows: ISACA.

ISACA. (2013). *Self-Assessment Guide: Using COBIT 5.* Rolling Meadows: ISACA.

ISACA. (2013). *Transforming Cybersecurity Using COBIT 5.* Rolling Meadows: ISACA.

PMBOK. (2013). *A Guide to the Project Management Body of Knowledge. Project Management Institute. 2013. p. 262. ISBN 978-1-935589-67-9.*

Suharyanto. (2019). *Indonesian CIO Network 7th Annual Bali Conference.* Bali: BSSN.