Penilaian Kapabilitas Tata Kelola Keamanan Teknologi Informasi dan Rekomendasi Perbaikan Menggunakan COBIT 5

Ade Dwi Andayani[1)], Obrina Candra Briliyant[2)]
(1) *Politeknik Siber dan Sandi Negara, ade.dwi@bssn.go.id*
(2) *Politeknik Siber dan Sandi Negara, obrina@poltekssn.ac.id*

Abstrak

Penilaian kapabilitas tata kelola Teknologi Informasi (TI) penting untuk dilakukan guna mengetahui kondisi penerapan tata kelola TI serta mengidentifikasi permasalahan kegiatan TI. Tata kelola keamanan teknologi informasi pada proses pengelolaan data yang kurang baik akan menimbulkan permasalahan yang merupakan kelemahan (vulnerabilities) sehingga dapat menimbulkan ancaman seperti kehilangan, pencurian, perusakan, dan penyadapan data penting perusahaan atau organisasi. Atas dasar tersebut, diperlukan penilaian kapabilitas tata kelola keamanan teknologi informasi untuk menghasilkan rekomendasi perbaikan sehingga proses pengelolaan data terhindar dari ancaman. Unit XYZ merupakan instansi pemerintah pengelola teknologi informasi di lingkungan instansi ABC. Layanan data berbasis teknologi informasi yang disediakan unit XYZ bersifat strategis. Dalam penelitian ini, dilakukan penilaian kapabilitas untuk mengetahui kondisi tata kelola keamanan TI organisasi saat ini. Selain itu disusun pula rekomendasi perbaikan tata kelola keamanan teknologi informasi menggunakan COBIT 5 serta ISO 27001:2013 dan ISO 27002:2013 pada unit XYZ. Proses pengumpulan data dengan cara wawancara, studi literatur, kuisioner dan observasi. Dari penelitian yang dilakukan, diketahui bahwa tata kelola keamanan TI pada unit XYZ berada pada level 0. Hasil penelitian berupa nilai kapabilitas dan rekomendasi tata kelola meliputi aspek struktur, proses, dan komunikasi internal.

Kata Kunci: COBIT 5 (1), ISO 27001 (2), ISO 27002 (3), keamanan TI (4), tata kelola (5).

1. PENDAHULUAN

Penilaian kapabilitas dilakukan untuk mengetahui kondisi sudah sejauh mana penerapan tata kelola teknologi informasi organisasi saat ini [1]. PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) mewajibkan Penyelenggara Sistem Elektronik dalam hal tata kelola menyediakan keamanan informasi terhadap jasa layanan Teknologi Informasi (TI) yang digunakan. Hal tersebut dilakukan guna menjamin setiap komponen dan keterpaduan seluruh sistem elektronik beroperasi sebagaimana mestinya [2]. Instansi ABC merupakan instansi pemerintah yang menyelenggarakan sistem elektronik untuk pelayanan publik. Instansi ABC mengesahkan peraturan tentang tata kelola teknologi informasi untuk mendukung tujuan penyelenggaraan pelayanan publik dan *good governance*.

Struktur tata kelola TI di instansi ABC terdiri dari atas Komite TI dan pengelola TI. Pengelola TI di lingkungan instansi ABC adalah unit XYZ. Menurut peraturan tata kelola teknologi informasi instansi ABC, pengelola TI memiliki tugas untuk melaksanakan tata kelola keamanan teknologi informasi. Menurut Kepala Bidang Infrastruktur Aplikasi dan Sistem Informasi (Kabid IASI) keamanan teknologi informasi akan berpengaruh pada kepercayaan (*trust*) dari *stakeholder* baik bagi unit XYZ maupun bagi instansi ABC. Hal tersebut dikarenakan data dan informasi yang dikelola unit XYZ harus memenuhi kaidah kebaruan, keakuratan, kerahasiaan, dan keamanan.

Pada penelitian ini, tata kelola teknologi informasi berfokus pada keamanan informasi. Hal ini dikarenakan teknologi dan informasi saling mengikat dalam proses bisnis organisasi. Kemudian dihadapkan dengan kebutuhannya untuk mengurangi risiko yang mencakup informasi dan aset TI dari ancaman yang terus berubah [3]. Menurut Kabid IASI, tata kelola keamanan teknologi informasi di Unit XYZ belum dilaksanakan secara optimal. Dalam rangka menerapkan tata kelola keamanan TI di unit XYZ, maka perlu dilakukan penilaian kapabilitas untuk mengetahui kondisi tata kelola keamanan TI organisasi saat ini. Hal ini dapat memudahkan untuk pemberian rekomendasi perbaikan tata kelola keamanan TI sesuai kebutuhan dan keadaan organisasi. Salah satu kerangka kerja yang dapat digunakan untuk menerapkan tata kelola keamanan TI adalah COBIT 5. Penilaian kapabilitas digunakan pedekatan COBIT 5 *Process Assessment Model* (PAM) [4].

Kerangka kerja COBIT 5 sudah digunakan dalam beberapa penelitian, yaitu penelitian Suryo Suminar [5] dengan melakukan evaluasi tata kelola keamanan teknologi informasi menggunakan COBIT 5 pada PPIKSN-BATAN dengan fokus proses APO13 dan DSS05. Tahapan penilaian kapabilitas yang dilakukan sesuai COBIT 5 *Assessment Programme Activities* yaitu *initiation, planning the assessment, data collection, data validation, data attribute level* dan *reporting the result*. Penelitian tersebut menghasilkan nilai kapabilitas dan rekomendasi perbaikan. Penelitian lainnya dilakukan oleh Raja Gantino Mufti [6] menggunakan COBIT 5 terhadap dua domain

proses yaitu APO13 dan DSS05 di PT Martina Berto yang menghasilkan *capability level* dan rekomendasi perbaikan menggunakan analisis SWOT dalam hal tata kelola fokus proses keamanan TI. Kedua penelitian tersebut memiliki tahapan penelitian yaitu penilaian kapabilitas, penentuan target, analisis kesenjangan dan penentuan rekomendasi.

Berdasarkan uraian di atas, maka pada penelitian ini akan dilakukan penilaian kapabilitas tata kelola keamanan teknologi informasi dan rekomendasi perbaikan di unit XYZ. Kerangka kerja yang digunakan pada penelitian ini yaitu COBIT 5 dengan fokus proses APO13 dan DSS05. Proses tersebut dipilih karena berkaitan dengan keamanan [7]. Perbedaan penelitian ini dengan penelitian sebelumnya [5][6] yaitu pada penelitian ini akan menggunakan kerangka kerja COBIT 5, ISO 27001 dan ISO 27002 sebagai tambahan rekomendasi. Selain itu, analisis SWOT dalam penelitian ini akan digunakan untuk memetakan kebutuhan organisasi mengenai tata kelola keamanan teknologi informasi. Hasil yang diharapkan dari penelitian ini yaitu berupa nilai kapabilitas dan rekomendasi tata kelola keamanan teknologi informasi di unit XYZ agar dapat diimplementasikan dalam mendukung tugas dan tanggung jawab sebagai pengelola TI di lingkungan instansi ABC.

2. LANDASAN TEORI

2.1 COBIT 5 PAM

Process Assessment Model merupakan model dasar untuk penilaian kapabilitas proses berdasarkan COBIT 5 sesuai dengan persyaratan ISO/IEC 15504-2 [4]. PAM merupakan proses kapabilitas dua dimensi yaitu proses dan kapabilitas. Dimensi pertama yaitu dimensi proses yang didefinisikan dan diklasifikasikan berdasarkan kategori proses. Dimensi kedua yaitu dimensi kapabilitas terdiri dari kumpulan atribut proses yang dikelompokkan ke dalam skala kapabilitas COBIT 5 PAM. Tabel 1 merupakan skala penilaian berdasarkan hasil pencapaian.

Tabel 1. Skala Penilaian

Kode	Deskripsi	Persentase pencapaian
N	*Not achieved*	0 - 15%
P	*Partially achieved*	> 15% - 50%
L	*Largely achieved*	> 50% - 85%
F	*Fully achieved*	> 85% - 100%

Adapun beberapa ketentuan dalam melakukan penilaian kapabilitas adalah sebagai berikut [8]:

- Penilaian dilakukan dengan mendefinisikan PRM yang mengacu pada COBIT 5 PAM
- Penilaian dimulai pada level 1 yang secara khusus mempunyai 1 indikator yaitu *performance indicator* (menggunakan *base practices* dan *work products*)
- Penilaian dilakukan dengan menggunakan skala N (0-15%), P (>15-50%), L (>50-85%), F (>85%-100%)
- Penilaian dapat dikatakan mencapai kapabilitas level apabila setidaknya nilai yang dicapai adalah L (>50-85%)
- Penilaian dapat dilakukan pada level selanjutnya jika pada level sebelumnya telah mencapai nilai F (>85%-100%).

2.2 Fokus Proses

Penelitian ini berfokus pada keamanan teknologi informasi. Oleh karena itu, tidak seluruh proses pada setiap domain dipilih untuk proses *assessment*. Proses yang dipilih dalam penelitian ini adalah APO13 dengan jumlah 3 sub-proses dan DSS05 dengan jumlah 7 sub-proses. Proses tersebut dipilih karena berkaitan dengan keamanan [9].

2.3 COBIT *Assessment Process Activities*

COBIT *Assessment Process Activities* menjelaskan proses penilaian yang termasuk di dalamnya adalah COBIT *Self Assessment Guide*, A *self-assessment tool kit*, COBIT *Assessor Guide*, COBIT *Process Assessment Model* (PAM) [4]. Berikut merupakan tahapan *Assessment Process Activities*:

1) *Initiation*
2) *Planning the assessment*
3) *Data collection*
4) *Data Validation*
5) *Data attribute level*
6) *Reporting the results*

2.4 Analisis SWOT

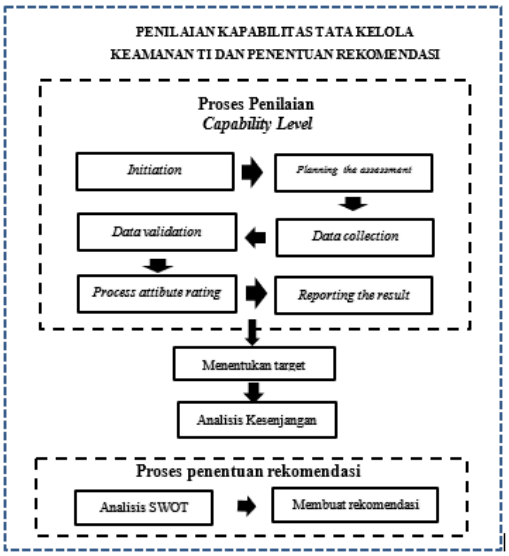
Analisis SWOT saat ini banyak digunakan untuk penyusunan perencanaan strategi bisnis yang bertujuan untuk menyusun strategi jangka panjang sehingga arah dan tujuan organisasi dapat tercapai dengan jelas dan dapat segera diambil keputusan [10]. Analisis ini didasarkan pada logika yang dapat memaksimalkan kekuatan (*Strength*) dan peluang (*Opportunities*), namun secara bersamaan dapat meminimalkan kelemahan (*Weakness*) dan ancaman (*Threats*). Pada penelitian ini analisis SWOT digunakan sebagai alat bantu dalam penyusunan rekomendasi.

3. METODOLOGI PENELITIAN

Pada penelitian ini dilakukan penilaian kapabilitas tata kelola keamanan TI di unit XYZ yang bertujuan untuk mengetahui *capability level* TI dalam pemanfaatan TI untuk menyediakan layanan publik. Metode kualitatif dipenelitian ini digunakan pada proses pengumpulan, penyajian, dan analisis data yang berkaitan dengan tata kelola keamanan TI di unit XYZ. Teknik pengumpulan data kualitatif pada penelitian ini yaitu observasi, wawancara, dan telaah

dokumentasi seperti pada peraturan internal Instansi ABC, peraturan eksternal, jurnal, buku, dan dokumen-dokumen lainnya yang terkait dengan penelitian. Selain itu digunakan teknik pengumpulan data kuantitatif berupa kuesioner sesuai dengan COBIT 5 *self assessment guide* untuk penentuan *capability level*.

Teknik analisis data yang akan digunakan dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Teknik analisis data

Sebelum melakukan penilaian kapabilitas, terlebih dahulu dilakukan pemetaan tujuan organisasi dengan *enterprise goals* COBIT. Berdasarkan Gambar. 1 secara umum tahapan analisis dari penilaian kapabilitas adalah sebagai berikut:

1. Penilaian kapabilitas dengan berdasarkan COBIT *Process Assessment Activities*
2. Menentukan target dengan metode wawancara berdasarkan nilai yang diperoleh saat ini.
3. Melakukan analisis kesenjangan dengan menentukan nilai upaya.
4. Penentuan rekomendasi digunakan analisis SWOT untuk memetakan kebutuhan organisasi.
5. Rekomendasi yang dihasilkan meliputi aspek struktur, proses dan komunikasi internal.

4. HASIL

4.1 Pemetaan Tujuan Organisasi

Indikator Kinerja Sasaran Kegiatan (IKSK) Unit XYZ dilakukan pemetaan terhadap *enterprise goals* yang terdapat pada COBIT 5. Pendekatan yang dilakukan adalah dengan melihat kesesuaian IKSK dengan *enterprise goals metrics* COBIT 5 *Enabling Process*. Dari hasil pemetaan diperoleh 8 *Enterprise Goals* yaitu:

1. EG 6, *Customer-oriented service culture*
2. EG 7, *Business service continuity and availability*
3. EG 11, *Optimisation of business process functionality*
4. EG 13, *Manages business change programmes*
5. EG 14, *Operational and staff productivity*
6. EG 15, *Compliance with internal policies*
7. EG 16, *Skilled and motivated people*
8. EG 17, *Product and business inovation culture*

Dari kedelapan *enterprise goals* terpilih, kemudian dilakukan pemetaan menjadi IT *related goals*. Pemetaan dilakukan dengan menggunakan *detail mapping enterprise goals to* IT-*related goals* COBIT 5 *Enabling Process*. Setelah pemetaan IT-*related goals* terhadap tujuan dan sasaran strategis sudah teridentifikasi, maka selanjutnya dilakukan pemetaan ke dalam COBIT 5 untuk menentukan proses yang didukung oleh IT-*related goals*. Proses APO13 dan DSS05 termasuk dalam *enabler process primary*.

4.2 Identifikasi Isu Permasalahan

Pada dasarnya, setiap organisasi memiliki kebutuhan dan permasalahan yang berbeda-beda. Permasalahan tersebut timbul akibat adanya keragaman latar belakang dan orientasi kebutuhan masing-masing organisasi. Berikut merupakan informasi mengenai isu permasalahan di Unit XYZ:

1. Hasil audit keamanan informasi yang menunjukkan hasil tidak layak,
2. Belum memiliki mekanisme pengelolaan risiko keamanan informasi,
3. Sumber daya manusia yang menangani keamanan informasi dan pengelolaan aset infrastruktur TI terbatas sebanyak 4 orang,
4. Belum terdapat unit khusus yang menangani keamanan informasi,
5. Proses tata kelola hanya sebatas praktik operasional organisasi tanpa adanya suatu kebijakan atau prosedur,
6. Proses penanganan insiden keamanan informasi masih belum formal dilakukan.

Permasalahan yang ada di Unit XYZ tersebut menunjukan terdapat kelemahan dalam hal tata kelola khususnya bidang keamanan TI. Kepala Unit XYZ menyatakan bahwa saat ini organisasi sedang mengupayakan perbaikan tata kelola TI, terlebih setelah dikeluarkannya kebijakan tata kelola TIK instansi ABC.

4.3 Penilaian Kapabilitas

a) *Initiation*

Berdasarkan tingkatan kewenangan instansi ABC, Unit XYZ memiliki posisi dan wewenang dalam melakukan tata kelola teknologi informasi di lingkungan internal instansi ABC [11]. Dari hasil wawancara diketahui bahwa Unit XYZ telah menerapkan beberapa sistem keamanan baik secara fisik maupun non fisik di antaranya adalah:

1) Keamanan fisik pada area *data center* meliputi *fingerprint* di pintu masuk utama ruang *data center*, ruang *server*, dan *meet me room*. Di dalam *meet me room* dilakukan proses *backup* dan

terdapat pula generator jika listrik mati. Di *meet me room* juga disimpan alat pemadam kebakaran FM200 *Fire Suppresion System.*

2) Penggunaan *Fortigate* 300D yang berfungsi sebagai *firewall*, *Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS). Fortigate 300D ini juga berfungsi sebagai *load balancer* untuk mengatur beban web.
3) Pengendalian *port* yang dapat mengakses jaringan dilakukan melalui *firewall.*
4) Keamanan dari serangan *malware* digunakan Kaspersky antivirus untuk perangkat *desktop*, sedangkan keamanan untuk *server* menggunakan Linux.
5) Jalur transmisi menggunakan *virtual private network* (VPN). Penggunaan *password* pada jalur VPN bersifat terbatas. Ketika ada pengembang pihak ketiga yang melakukan perbaikan jaringan, maka *password* akan segera diganti.

Namun sistem pengamanan informasi tersebut masih belum maksimal. Hal ini dikarenakan pada kenyataannya, proses penanganan insiden keamanan informasi Unit XYZ belum secara formal dilakukan. Selain itu, Standar Operasional Prosedur (SOP) terkait pengelolaan TI belum secara formal dibentuk. Keamanan teknologi informasi yang saat ini diterapkan tidak memiliki pedoman tertentu dalam penyelenggaraannya. Menurut Rencana Strategis, penerapan teknologi di Unit XYZ membutuhkan norma, standar, prosedur, dan kriteria (NSPK) serta kebijakan untuk pengimplementasiannya [11].

b) *Planning the Assessment*

Sebelum melakukan penilaian kapabilitas, perlu dilakukan perencanaan penilaian. Tahap perencanaan dilakukan untuk menentukan responden. Responden ditentukan dengan teknik *purposive sampling* berdasarkan RACI *chart* COBIT 5 *Enabling Process*. Parameter yang digunakan dalam menentukan responden yaitu *responsible* dan *accountable*. *Key management practice* yang memiliki jumlah parameter *responsible* dan *accountable* terbanyak dipilih menjadi responden. Responden setiap *enabler process* dapat berbeda.

Berdasarkan RACI *chart* APO13 dan DSS05 terdapat beberapa *role* yang berperan sebagai responden. *Role* tersebut diantaranya *Chief Information Security Officer* (CISO), *Chief Information Officer* (CIO), *Information Security Manager* (ISM), *Head* IT *Operation*, *Head IT Administration*. Kemudian dilakukan padanan jabatan antara *role*/*structure* COBIT dengan jabatan di Unit XYZ. Tabel 2 merangkum responden yang berperan untuk melakukan penilaian kapabilitas setiap proses.

c) *Data collection*

Langkah ini dilakukan dengan menilai setiap atribut pada masing-masing *enabler process* sesuai dengan COBIT 5 PAM. Hasil rekapitulasi penilaian kapabilitas proses terhadap masing-masing 3 narasumber dapat dilihat pada Tabel 3.

Tabel 2. Daftar responden

Proses	Responden
APO13 *Manage Security*	1. Kepala Unit XYZ 2. Kabid Infrastruktur, Aplikasi dan Sistem Informasi 3. Kasubbid Aplikasi dan Sistem Informasi
DSS05 *Manage Security Services*	1. Kepala Unit XYZ 2. Kabid Infrastruktur, Aplikasi dan Sistem Informasi 3. Kasubbid Jaringan dan Sarana

Tabel 3. Rekapitulasi penilaian proses APO13

Responden 1

No	*Outcome*	*Base Practice*		*Work Product*		Total
		Kode	Nilai	Kode	Nilai	
1	APO13-01	APO13-BP1	44 %	APO13-WP1 APO13-WP2	20%	32%
2	APO13-02	APO13-BP2	29 %	APO13-WP3 APO13-WP4	12%	21%
3	APO13-03	APO13-BP3	29 %	APO13-WP5 APO13-WP6	32%	26%
					Persentase akhir	26%

Responden 2

No	*Outcome*	*Base Practice*		*Work Product*		Total
		Kode	Nilai	Kode	Nilai	
1	APO13-01	APO13-BP1	52 %	APO13-WP1 APO13-WP2	15%	33%
2	APO13-02	APO13-BP2	30 %	APO13-WP3 APO13-WP4	60%	45%
3	APO13-03	APO13-BP3	22 %	APO13-WP5 APO13-WP6	50%	36%
					Persentase akhir	38%

Responden 3

No	*Outcome*	*Base Practice*		*Work Product*		Total
		Kode	Nilai	Kode	Nilai	
1	APO13-01	APO13-BP1	14 %	APO13-WP1 APO13-WP2	10%	12%
2	APO13-02	APO13-BP2	15 %	APO13-WP3 APO13-WP4	22%	18%
3	APO13-03	APO13-BP3	7%	APO13-WP5 APO13-WP6	15%	11%
					Persentase akhir	14%

Kemudian dilakukan pula rekapitulasi terhadap penilaian kapabilitas proses DSS05 yang dapat dilihat pada Tabel 4.

Dari Tabel 3 dan Tabel 4 dapat dilihat bahwa penilaian proses APO13 yang diberikan oleh responden berturut-turut adalah 26%, 38% dan 14%. Sedangkan penilaian proses DSS05 yang diberikan oleh responden berturut-turut adalah 33%, 38% dan 62%. Pencapaian setiap *outcome* dinilai dari pelaksanaan *base practice* dan pencapaian *output* sesuai dengan parameter yang telah didefinisikan. Nilai tersebut diperoleh berdasarkan penilaian responden. Untuk mendapatkan persentase *outcome* adalah dengan menghitung rata-rata persentase dari *base practice* dan *work product*. Persentase *base practice* diperoleh dari rata-rata aktivitas yang telah dilakukan. Persentase *work product* diperoleh dari rata-rata pencapaian *output*. Persentase akhir diperoleh dengan menghitung rata-rata nilai persentase *outcome*.

Tabel 4. Rekapitulasi penilaian proses DSS05

Responden 1						
No	***Outcome***	***Base Practice***		***Work Product***		**Total**
		Kode	**Nilai**	**Kode**	**Nilai**	
1	DSS05-01	DSS05-BP1	44%	DSS05-WP1 DSS05-WP2	20%	12%
		DSS05-BP2	36%	DSS05-WP3 DSS05-WP4	10%	
		DSS05-BP7	21%	DSS05-WP10 DSS05-WP11 DSS05-WP12	12%	
2	DSS05-02	DSS05-BP1	50%	DSS05-WP1 DSS05-WP2	5%	28%
		DSS05-BP3	56%	DSS05-WP5	5%	
3	DSS05-03	DSS05-BP4	54%	DSS05-WP6 DSS05-WP7	15%	34%
4	DSS05-04	DSS05-BP5	64%	DSS05-WP8 DSS05-WP9	20%	23%
5	DSS05-05	DSS05-BP6	27%	DSS05-WP13 DSS05-WP14	20%	23%
					Persentase akhir	33%

Responden 2						
No	***Outcome***	***Base Practice***		***Work Product***		**Total**
		Kode	**Nilai**	**Kode**	**Nilai**	
1	DSS05-01	DSS05-BP1	64%	DSS05-WP1 DSS05-WP2	15%	43%
		DSS05-BP2	69%	DSS05-WP3 DSS05-WP4	32%	
		DSS05-BP7	65%	DSS05-WP10 DSS05-WP11 DSS05-WP12	15%	
2	DSS05-02	DSS05-BP1	64%	DSS05-WP1 DSS05-WP2	15%	41%
		DSS05-BP3	73%	DSS05-WP5	15%	
3	DSS05-03	DSS05-BP4	36%	DSS05-WP6 DSS05-WP7	32%	34%
4	DSS05-04	DSS05-BP5	68%	DSS05-WP8 DSS05-WP9	50%	59%
5	DSS05-05	DSS05-BP6	15%	DSS05-WP13 DSS05-WP14	15%	15%
					Persentase akhir	38%

Responden 3						
No	***Outcome***	***Base Practice***		***Work Product***		**Total**
		Kode	**Nilai**	**Kode**	**Nilai**	
1	DSS05-01	DSS05-BP1	82%	DSS05-WP1 DSS05-WP2	10%	44%
		DSS05-BP2	79%	DSS05-WP3 DSS05-WP4	12%	
		DSS05-BP7	73%	DSS05-WP10 DSS05-WP11 DSS05-WP12	12%	
2	DSS05-02	DSS05-BP1	82%	DSS05-WP1 DSS05-WP2	10%	43%
		DSS05-BP3	74%	DSS05-WP5	8%	
3	DSS05-03	DSS05-BP4	74%	DSS05-WP6 DSS05-WP7	55%	64%
4	DSS05-04	DSS05-BP5	84%	DSS05-WP8 DSS05-WP9	80%	82%
5	DSS05-05	DSS05-BP6	73%	DSS05-WP13 DSS05-WP14	80%	76%
					Persentase akhir	62%

d) *Data validation*

Pada tahap *data validation* dilakukan verifikasi melalui wawancara dan observasi terhadap hasil kuesioner yang telah diperoleh dari narasumber yang dijadikan responden. Hal ini dilakukan untuk menggali informasi secara lebih mendalam dan sebagai bahan analisis terhadap hasil kuesioner. Proses verifikasi dilakukan dengan cara menganalisis *work product* dan *base practice* dalam mencapai *outcome* pada masing-masing proses.

e) *Data attribute level*

Pada tahap ini dilakukan analisis pencapaian setiap atribut pada masing-masing proses. *Data attribute level* dilakukan berdasarkan data yang telah divalidasi. Tahap ini memiliki hubungan antara nilai kapabilitas yang telah diperoleh dengan hasil observasi pada tahap *data validation*. Tabel 5 di bawah ini merupakan pembahasan mengenai hasil pengukuran tingkat kapabilitas pada proses APO13 dan DSS05.

Tabel 5. *Data attribute level* APO13 dan DSS05

Responden 1										
Process Name	**Level 0**	**Level 1**	**Level 2**		**Level 3**		**Level 4**		**Level 5**	
Attributes	*False if Capability Level ≥1*	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	TRUE	P (26%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)
DSS05	TRUE	P (33%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)

Responden 2										
Process Name	**Level 0**	**Level 1**	**Level 2**		**Level 3**		**Level 4**		**Level 5**	
Attri-butes	*False if Capability Level ≥1*	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	TRUE	P (38%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)
DSS05	TRUE	P (38%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)

Responden 3										
Process Name	**Level 0**	**Level 1**	**Level 2**		**Level 3**		**Level 4**		**Level 5**	
Attri-butes	*False if Capability Level ≥1*	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	TRUE	N (14%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)
	TRUE	P (62%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)	N (0%)

Berdasarkan Tabel 5 dapat dilihat hasil penilaian proses APO13 dan DSS05 menunjukkan hasil 2 dari

3 responden menunjukkan nilai 'P' yang menunjukkan bahwa pencapaian kapabilitas yang diperoleh adalah 0. Hal tersebut menjelaskan bahwa implementasi proses telah sebagian dilakukan namun gagal mencapai *outcome* dari proses. Dari hasil observasi ditemukan bahwa Unit XYZ telah melaksanakan beberapa *base practice* dalam penerapan SMKI, namun *output* proses belum tercapai. Selain itu dari hasil observasi ditemukan bahwa Unit XYZ telah melaksanakan beberapa praktik operasional dalam mekanisme keamanan jaringan dan pengaturan hak akses terhadap *server*/*storage*. Akan tetapi standar, prosedur dan kebijakan pengelolaan masih belum ada.

f) *Reporting the result*

Hasil rekapitulasi penilaian terhadap masing-masing proses disajikan dan didokumentasikan sesuai dengan penilaian responden. Pada tahap ini dilakukan pelaporan hasil akhir penilaian yang berisi penentuan tingkat kemampuan saat ini. Pencapaian level kapabilitas proses terhadap 3 responden dapat dilihat pada Tabel 6.

Tabel 6. Level proses APO13 dan DSS05

No	Proses COBIT yang dinilai	Responden	Level Kapabilitas					
			0	1	2	3	4	5
1	APO13 *Manage security*	Responden 1	√					
		Responden 2	√					
		Responden 3	√					
2	DSS05 *Manage security service*	Responden 1	√					
		Responden 2	√					
		Responden 3		√				

Dari Tabel 6 dapat disimpulkan bahwa pada proses APO13 ketiga responden menentukan level kapabilitas yaitu 0. Pada proses DSS05 sebanyak dua responden menentukan level kapabilitas pada level 0 dan satu responden menentukan level 1. Oleh karena level kapabilitas dua dari tiga responden menunjukkan level 0 maka disimpulkan bahwa proses DSS05 berada pada level 0.

4.4 Penentuan Target

Penentuan target dilakukan melalui wawancara dengan Kepala Unit XYZ. Hal tersebut dilakukan karena Kepala Unit XYZ merupakan pejabat paling senior di organisasi yang bertanggung jawab atas keamanan informasi organisasi dalam segala bentuknya. Dari hasil wawancara diketahui bahwa target level yang hendak dicapai oleh Unit XYZ adalah 1 pada seluruh proses. Hal ini berarti organisasi menghendaki rekomendasi perbaikan berada satu level di atasnya.

4.5 Analisis Kesenjangan

Analisis kesenjangan dilakukan antara pencapaian level kapabilitas yang diperoleh Unit XYZ saat ini dengan target yang diharapkan. Semakin besar gap yang terjadi maka semakin besar upaya yang dibutuhkan organisasi untuk melaksanakan perbaikan. Perhitungan nilai upaya dilakukan terhadap 3 responden (R) pada masing-masing proses. Penghitungan nilai upaya setiap proses dijelaskan melalui Tabel 7 berikut.

Tabel 7. Analisis kesenjangan

APO13						
No	Responden	Level saat ini	Pencapaian indikator (%)	Tar-get	Gap	Nilai upaya
A	B	C	D	E	F	G
1	R 1	0	26%	1	1	1,74
2	R 2	0	38%	1	1	1,62
3	R 3	0	14%	1	1	1,86
DSS05						
No	Responden	Level saat ini	Pencapaian indikator (%)	Tar-get	Gap	Nilai upaya
A	B	C	D	E	F	G
1	R1	0	33%	1	1	1,67
2	R2	0	38%	1	1	1,62
3	R3	1	62%	1	0	0,38

Nilai upaya yang telah diperoleh dilakukan analisis sehingga dapat ditentukan prioritas proses. Analisis nilai upaya dapat dilihat pada Tabel 8.

Tabel 8. Analisis Perbandingan nilai upaya

Responden	APO13	DSS05	Perbandingan nilai upaya
R 1	1,74	1,67	APO13 > DSS05
R 2	1,62	1,62	APO13 = DSS05
R 3	1,86	0,38	APO13 > DSS05

Berdasarkan Tabel 8, data analisis perbandingan diperoleh hasil 2 dari 3 responden menunjukkan bahwa proses APO13 memiliki nilai upaya lebih besar daripada proses DSS05. Oleh karena proses DSS05 memiliki nilai upaya yang lebih kecil dari proses APO13, maka tujuan proses DSS05 lebih mudah tercapai daripada APO13.

4.6 Penentuan Rekomendasi

Rekomendasi dapat disusun dengan terlebih dahulu melakukan analisis SWOT terhadap proses tata kelola keamanan TI di Unit XYZ . Tabel 9 merupakan hasil pemetaan strategi SWOT.

Hasil analisis faktor eksternal dan internal yang meliputi aspek kekuatan (*strength*), kelemahan (*weakness*), peluang (*opportunity*), dan ancaman (*threat*) kemudian dilakukan pemetaan terhadap matriks Kearns menghasilkan isu-isu strategis organisasi. Hasil matriks analisis SWOT ini akan digunakan sebagai dasar pemetaan prioritas rekomendasi.

Dalam rangka meningkatkan upaya perbaikan tata kelola keamanan teknologi informasi, maka diberikan rekomendasi meliputi 3 aspek tata kelola yaitu struktur, proses, dan komunikasi. Mekanisme tersebut bertujuan untuk menerapkan tata kelola TI yang efektif [12].

Tabel 9. Analisis SWOT

Eksternal	*Opportunity* (O)	*Threats* (T)
Strength (S)	1. Menyusun kebijakan SMKI untuk meningkatkan kinerja organisasi dan nilai Indeks KAMI 2. Meningkatkan peraturan terkait kepatuhan keamanan informasi bagi pegawai 3. Membentuk kebijakan dan prosedur pengelolaan perangkat jaringan. 4. Melaksanakan manajemen risiko terhadap aset informasi dari kemungkinan malware. 5. Membuat kebijakan manajemen log akses terhadap informasi berklasifikasi 6. Meningkatkan intensitas diselenggarakan pelatihan keamanan informasi 7. Meningkatkan intensitas uji penetrasi minimal 3 bulan sekali 8. Melakukan rencana pengembangan TI dari hasil peninjauan insiden keamanan informasi 9. Membuat prosedur resmi terdokumentasi terkait akses ke infrastruktur TI 10. Melakukan analisis risiko terhadap sistem komputer agar pengamanan yang diterapkan tepat sasaran	1. Komite TI menyusun program kerja untuk meningkatkan kinerja dalam pemberian layanan 2. Membuat kebijakan larangan menggunakan perangkat lunak yang tidak resmi bagi pegawai. 3. Meningkatkan pengelolaan dan pengawasan penggunaan *firewall* 4. Melakukan *scanning* dan *update* antivirus secara berkala 5. Meningkatkan pengawasan log akses jaringan VPN dari penyalahgunaan pihak yang tidak berhak 6. Meningkatkan intensitas uji penetrasi aplikasi dalam satu tahun 7. Meningkatkan fungsi API WSO2. 8. Melakukan pemutakhiran sistem operasi *server* dan *desktop* secara berkala 9. Melakukan update perkembangan perangkat lunak berbahaya agar mekanisme perlindungan disesuaikan
Weakness (W)	1. Menyusun rencana pembentukan unit khusus yang menangani masalah keamanan informasi 2. Membentuk tim ad hoc yang sudah tesrertifikasi untuk menangani permasalahan keamanan informasi 3. Melakukan manajemen risiko 4. Menyusun rencana peningkatan dan pengembangan keamanan informasi 5. Melakukan sosialisasi dan pelatihan keamanan informasi secara merata bagi pegawai 6. Membentuk dan mengesahkan kebijakan SMKI 7. Membentuk prosedur akses fisik ke infrastruktur TI sesuai kebutuhan kerja 8. Melakukan manajemen risko keamanan informasi untuk melakukan klasifikasi data 9. Menetapkan mekanisme *penetration testing* berkala pada jaringan 10. Melakukan pelatihan tentang *malware* secara merata bagi pegawai	1. Membentuk tim khusus yang menangani masalah serangan terhadap server. 2. Melakukan kajian mengenai malware dan menerapkan upaya peningkatan pengamanan. 3. Meningkatkan pelatihan keamanan informasi sehingga dapat mendeteksi serangan ke sistem 4. Membuat prosedur pencegahan malware dengan membatasi penggunaan perangkat lunak bajakan

a) Struktur

Dari analisis struktur organisasi yang ada di Unit XYZ dengan segala tugas pokok dan fungsinya dipetakan kepada deskripsi *role* COBIT, diperoleh hasil bahwa terdapat fungsi tambahan untuk membantu mengoptimalkan kinerja tata kelola. Rekomendasi dari aspek struktur ini diharapkan dapat menjadi pertimbangan bagi organisasi untuk meningkatkan tata kelola. Rekomendasi struktur organisasi dapat dilihat pada Tabel 10.

Tabel 10.Rekomendasi tambahan fungsi peran COBIT

COBIT 5 *role*	Deskripsi
Steering Comittee	Sekelompok pemangku kepentingan dan ahli yang bertanggung jawab untuk pedoman program dan proyek, termasuk pengelolaan dan pemantauan rencana, alokasi sumber daya, penyampaian nilai dan manfaat, serta manajemen program dan risiko proyek
Programme and Project Management Office (PMO)	Fungsi yang bertanggung jawab untuk mendukung program dan manajer proyek, mengumpulkan, menilai dan memberi nasihat tentang peluang investasi dan kasus bisnis merekomendasikan metode dan kontrol tata kelola/manajemen, serta pelaporan tentang kemajuan dalam mempertahankan dan menciptakan nilai dari investasi dan layanan
Compliance	Fungsi dalam organisasi yang bertanggung jawab terkait pedoman hukum, peraturan dan kepatuhan terhadap kontrak
Audit	Fungsi dalam organisasi yang bertanggung jawab dalam hal audit internal

b) Proses

Dari hasil penilaian kapabilitas ditentukan rekomendasi berdasarkan COBIT 5 dan ISO 27002. Oleh karena target level organisasi adalah level 1, maka rekomendasi COBIT 5 disusun berdasarkan *Base Practice* (BP) dan *Work Product* (WP). ISO 27001:2013 dan ISO 27002:2013 digunakan sebagai tambahan rekomendasi yang menjelaskan pedoman implementasi. Rekomendasi yang dihasilkan baik COBIT maupun ISO 27001 dan ISO 27002 kemudian dipetakan terhadap strategi yang telah diperoleh pada Tabel 9. Strategi tersebut dapat digunakan sebagai gambaran bagi organisasi untuk meningkatkan nilai dengan memanfaatkan peluang, memperlunak ancaman, memaksakan peluang, dll. Hasil pertemuan antara faktor eksternal dan internal akan memberikan beberapa kondisi diantaranya:

- *Comparative advantage* (S,O) − kemungkinan bagi organisasi untuk bisa berkembang lebih cepat.
- *Mobilization* (S,T) −mobilisasi sumber daya yang merupakan kekuatan organisasi untuk memperlunak ancaman, merubah ancaman itu menjadi sebuah peluang.
- *Divestment* (W,O) − keinginan memanfaatkan peluang, namun tidak ada kekuatan sehingga

pilihannya melepas peluang atau memaksakan peluang.

- *Damage control* (W,T) − mengendalikan kerugian sehingga tidak lebih parah dari yang diperkirakan.

Prioritas rekomendasi yang telah dipetakan dengan strategi dari analisis SWOT dapat dilihat pada Tabel 11.

Tabel 11. Prioritas rekomendasi

No	Prioritas Rekomendasi	Strategi	Keterangan
1	**5.1.1 *Policies for information security* (ISO 27002:2013)** Membuat kebijakan keamanan informasi yang menyebutkan persyaratan strategi bissnis; peraturan perundang-undangan; ancaman keamanan informasi terkini	• Menyusun kebijakan SMKI untuk meningkatkan kinerja organisasi dan nilai Indeks KAMI • Membentuk dan mengesahkan kebijakan SMKI	*Comparative advantage* dan *Divestment*
2	**6.1.1 *Information security roles and responsibilities* (ISO 27002:2013)** Mengalokasikan tanggung jawab perlindungan aset individu dan pendelegasiannya	Membentuk tim *ad hoc* yang sudah tersertifikasi untuk menangani permasalahan keamanan informasi	*Divestment*
3	**8.2 *Information security risk assessment* (ISO 27001:2013)** Melakukan penilaian risiko keamanan informasi pada rentang waktu yang terencana dengan mempertimbangkan kriteria yang telah ditetapkan	• Melakukan manajemen risiko • Melakukan manajemen risko keamanan informasi untuk melakukan klasifikasi data	*Divestment*
4	**7.2 *Competence* (ISO 27001:2013)** Penyediaan pelatihan, bimbingan, atau penugasan terhadap karyawan yang kompeten	• Meningkatkan intensitas diselenggarakan pelatihan keamanan informasi • Meningkatkan pelatihan keamanan informasi sehingga dapat mendeteksi serangan ke sistem • Melakukan sosialisasi dan pelatihan keamanan informasi secara merata bagi pegawai	*Comparative* advantage, *Divestment*, dan *Damage* control
5	**12.2.1 *Control against malware* (ISO 27002:2013)** Membuat kebijakan resmi yang melarang penggunaan perangkat lunak tidak sah	• Membuat kebijakan larangan menggunakan perangkat lunak yang tidak resmi bagi pegawai • Membuat prosedur pencegahan malware dengan membatasi penggunaan perangkat lunak bajakan	*Mobilization* dan *Damage control*
6	**12.2.1 *Control against malware* (ISO 27002:2013)** Mempersiapkan rencana berkesinambungan untuk pemulihan dari serangan *malware*	• Melakukan kajian mengenai *malware* dan menerapkan upaya peningkatan pengamanan • Melakukan *update* perkembangan perangkat lunak berbahaya agar mekanisme perlindungan disesuaikan	*Mobilization* dan *Damage control*
7	**13.1.1 *Network controls* (ISO 27002:2013)** Membuat prosedur pengelolaan peralatan jaringan	Membentuk kebijakan dan prosedur pengelolaan perangkat jaringan	*Comparative advantage*
8	**COBIT 5** Melakukan pengujian penetrasi secara berkala untuk menentukan kecukupan perlindungan jaringan	• Menetapkan mekanisme *penetration testing* berkala pada jaringan • Meningkatkan intensitas uji penetrasi minimal 3 bulan sekali	*Comparative advantage* dan *Divestment*
9	**11.2 *Equipment* (ISO 27002:2013)** Membuat kebijakan keamanan perangkat	Melakukan analisis risiko terhadap sistem komputer agar pengamanan yang diterapkan tepat sasaran	*Comparative advantage*
10	**9.1.2 *Access network and network services* (ISO 27002:2013)** Membuat kebijakan keamanan perangkat pada layanan jaringan	Melakukan pemutakhiran sistem operasi *server* dan *desktop* secara berkala	*Mobilization*
11	**9.1.1 *Access control policy* (ISO 27002:2013)** Membuat kebijakan akses kontrol secara tepat dan pembatasan sesuai pengguna tetentu	• Meningkatkan pengawasan *log* akses jaringan VPN dari penyalahgunaan pihak yang tidak berhak • Membuat kebijakan manajemen *log* akses terhadap informasi berklasifikasi	*Comparative advantage* dan *mobilization*
12	**9.4.1 *Information access restriction* (ISO 27002:2013)** Melakukan pembatasan akses terhadap sistem informasi dan aplikasi sesuai dengan kebijakan akses kontrol	Melakukan manajemen risko keamanan informasi untuk melakukan klasifikasi data	*Divestment*
13	**11.1.2 *Physical entry control* (ISO 27002:2013)** Membuat kebijakan kontrol masuk secara fisik terhadap area TI	• Membuat prosedur resmi terdokumentasi terkait akses ke infrastruktur TI • Membentuk prosedur akses fisik ke infrastruktur TI sesuai kebutuhan kerja	*Comparative advantage* dan *Divestment*
14	**2.3 *Handling of assets* (ISO 27002:2013)** Membuat prosedur untuk menangani aset sesuai dengan klasifikasi informasi organisasi	Melakukan manajemen risko keamanan informasi untuk melakukan klasifikasi data	*Divestment*
15	**12.4.1 *Event logging* (ISO 27002:2013)** Membuat dan meninjau secara berkala *log* peristiwa yang mencatat aktivitas pengguna	Membuat kebijakan manajemen log akses terhadap informasi berklasifikasi	*Comparative advantage*

Tabel 12. Rekomendasi program kerja

No	Kelemahan/ *weakness*	Program kerja
1	Kebijakan	• Menentukan ruang lingkup dan batasan SMKI sesuai strategi bisnis • Melakukan penilaian risiko keamanan informasi untuk memeperoleh profil risiko keamanan informasi unit XYZ • Membuat kebijakan yang melarang penggunaan perangkat lunak bajakan bagi karyawan • Membuat kebijakan *update* antivirus secara berkala • Memetakan tanggung jawab penanganan terhadap *malware* • Melakukan penilaian risiko terhadap peralatan jaringan • Membuat prosedur pengelolaan peralatan jaringan • Membentuk tim untuk mengelola *role authorization* dan *remote access* pada aplikasi dan jaringan • Membuat kebijakan kontrol akses untuk jaringan dan layanan jaringan • Membuat hak akses istimewa untuk pengguna tertentu sesuai kepentingan • Menentukan batasan perimeter akses terhadap area yang terdapat informasi sensitif • Membuat pedoman petunjuk teknis terkait akses terhadap aset TI • Membuat prosedur dan petunjuk teknis untuk menangani aset TI sesuai klasifikasi informasi unit XYZ
2	Manajemen	• Menentukan peran dan tanggung jawab pengelolaan keamanan informasi secara umum dan spesifik • Melakukan pemetaan alokasi tanggung jawab perlindungan aset dan pendelegasiannya • Memelihara arsitektur untuk mengelola risiko terkait keamanan • Membentuk tim audit internal yang bertanggung jawab meninjau SMKI • Melakukan pembatasan akses terhadap sistem informasi dan aplikasi sesuai dengan fungsi kerja di unit XYZ Menetapkan prosedur pencatatan insiden keamanan informasi yang meliputi aktivitas pengguna, kesalahan, dan peristiwa keamanan informasi • Menetapkan daftar informasi log yang harus diberikan pelindungan
3	Akuntabilitas	• Menetapkan jadwal uji penetrasi jaringan secara berkala • Membuat laporan hasil uji penetrasi • Melakukan enkripsi pada *database* penyimpanan • Melakukan enkripsi jaringan komunikasi
4	Kompetensi dan SDM	• Membuat jadwal pelatihan kesadaran keamanan informasi secara berkala bagi karyawan • Mengembangkan program pendidikan dan pelatihan keamanan informasi dengan pertimbangan informasi unit XYZ yang akan dilindungi • pelatihan berkala untuk pencegahan *malware* • Melaksanakan pelatihan bagi *programmer* untuk pemulihan serangan *malware*

Untuk mendukung rekomendasi proses yang telah disebutkan di atas, maka disusun suatu program kerja yang direncanakan terealisasi hingga tahun 2020 untuk unit XYZ. Rekomendasi program kerja dapat dilihat pada Tabel 12**.** Secara umum terdapat 27 program kerja yang diusulkan meliputi kebijakan, manajemen, akuntabilitas, kompetensi dan SDM.

c) Komunikasi Internal

Rekomendasi pada aspek struktur dan proses perlu dikomunikasikan kepada seluruh komponen organisasi. Rekomendasi strategi komunikasi internal Unit XYZ dengan menggunakan salah satu tahap manajemen perubahan Kotter. Tahapan tersebut adalah mengomunikasikan visi yang telah dibentuk kepada seluruh elemen organisasi. Strategi komunikasi internal ini dibentuk dalam sebuah program kerja. Usulan program kerja terkait strategi komunikasi internal dapat dilihat pada Tabel 13.

Tabel 13. Rekomendasi program kerja strategi komunikasi internal

No	Program Kerja	Penanggung jawab
1	Sosialisasi langsung secara rutin terhadap pegawai mengenai suatu kebijakan yang telah ditentukan oleh organisasi	Kabid Infrastruktur, Aplikasi dan Sistem Informasi
2	Pemanfaatan *newsletter* melalui email untuk pemberitahuan kebijakan baru	Kasubbag Persuratan dan Kepegawaian
3	Membuat agenda pertemuan secara teratur dengan karyawan terkait pemahaman status pekerjaan, proyek, tim atau organisasi secara keseluruhan	Kepala Unit XYZ

5. SIMPULAN DAN SARAN

5.1 Simpulan

Kesimpulan yang didapatkan berdasarkan hasil penelitian yang telah dilakukan yaitu:

a. Penilaian kapabilitas terhadap tata kelola keamanan TI di Unit XYZ dari 3 responden menghasilkan nilai 26%, 38%, dan 14% pada *enabler process* APO13 serta 33%, 38%, dan 62% pada *enabler process* DSS05. Nilai tersebut belum memenuhi untuk pencapaian level 1. Sehingga proses APO13 dan DSS05 disimpulkan berada pada level 0. Hasil penilaian tersebut menunjukkan bahwa tata kelola keamanan TI belum mencapai *outcome* dan tujuan dari masing-masing proses belum terpenuhi.
b. Target level yang hendak dicapai oleh Unit XYZ yaitu level 1. Perhitungan nilai upaya terhadap penilaian masing masing responden pada proses APO13 adalah 1,74; 1,62; dan 1,86. Pada proses DSS05 diperoleh nilai upaya masing masing responden sebesar 1,67; 1,62; 0,38. Dari hasil analisis diperoleh informasi bahwa 2 dari 3 responden menunjukkan nilai upaya proses DSS05 lebih kecil dibandingkan APO13. Oleh karena itu proses DSS05 lebih mudah untuk

mencapai tujuan proses dibandingkan proses APO13.

c. Dari hasil penilaian kapabilitas ditentukan rekomendasi berdasarkan COBIT 5 dan ISO 27002. Aspek tersebut diantaranya kebijakan, manajemen, sumber daya manusia dan akuntablitas. Terdapat 15 rekomendasi prioritas hasil pemetaan dengan strategi analisis SWOT. Selain itu, rekomendasi juga disusun dalam bentuk program kerja. Rekomendasi program kerja berjumlah 27 meliputi aspek kebijakan, manajemen, sumber daya manusia dan akuntabilitas serta 3 strategi komunikasi internal.

5.2 Saran

Berdasarkan hasil penelitian ini, terdapat saran yaitu hasil rekomendasi tata kelola keamanan TI di Unit XYZ dapat ditindaklanjuti dengan membentuk kebijakan Sistem Manajemen Keamanan Informasi berbasis risiko sebagai fokus utama.

REFERENSI

[1] A. Haryanti, "Pengukuran Tingkat Kapabilitas Tata Kelola Teknologi Informasi dan Rekomendasi Perbaikan Berdasarkan Kerangka Kerja COBIT 5 Studi Kasus Badan Kepegawaian Negara," Universitas Indonesia, 2015.

[2] Republik Indonesia, "Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik." 2012.

[3] Kemenristekdikti, "Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Nomor 15 Tahun 2015 tentang Organisasi dan Tata Kerja Kementerian Riset, Teknologi dan Pendidikan Tinggi." 2015.

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

[5] S. Suminar, "Evaluation of Information Technology Governance using COBIT 5 Framework Focus APO13 dan DSS05 in PPIKSN-BATAN," *IEEE*, 2014.

[6] R. G. Mufti and Y. T. Mursityo, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk)," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, pp. 1622–1631, 2017.

[7] ISACA, "COBIT 5 for Information Security." ISACA, Rolling Meadows, 2012.

[8] R. A. Ashari, "Rencana Penerapan Cyber-risk Management Menggunakan NIST Cyber Security Framework (CSF) for Improving Critical Infrastructure dan COBIT 5 (Studi Kasus: Sistem Informasi XYZ)," Sekolah Tinggi Sandi Negara, 2018.

[9] ISACA, "COBIT 5 Enabling Processes." ISACA, Rolling Meadows, 2012.

[10] F. Rangkuti, *Analisis SWOT: Teknik Membedah Kasus Bisnis*. Jakarta: PT. Gramedia, 2006.

[11] Kemenristekdikti, "Revitalisasi Rencana Strategis Pusat Data dan Informasi Ilmu Pengetahuan, Teknologi, dan Pendidikan Tinggi 2016-2019." Kemenristekdikti, 2016.

[12] Y. Supriyadi, "Design of IT Governance Implementation Mechanism Using Organization Diagnosis and COBIT 5," *Open Access J. Inf. Syst.*, 2015.