Penilaian Tata Kelola Keamanan Informasi Perpustakaan dengan Framework Cobit 5

Studi Kasus Dinas Perpustakaan dan Arsip Kota Bandung

Yoki Muchsam
Jurusan Teknik Komputer
STMIK AMIK Bandung
Jl. Jakarta 28 Bandung
yockie.muchsam@gmail.com

Abstrak— Dinas Perpustakaan dan Arsip Daerah Kota Bandung (Dispusip). Dispusip membutuhkan Tata Kelola Keamanan Informasi yang baik agar dapat meningkatkan pelayanannya terhadap masyarakat. Memanfaatkan Teknologi Informasi Perpustakaan dalam tiga tingkatan yaitu memberikan dukungan untuk pelayanan Perpustakaan, sebagai alat bantu pengelolaan perpustakaan dan sarana komunikasi serta pemanfaatan teknologi informasi untuk membantu pengambilan keputusan. Tujuan penelitian ini adalah melakukan penilaian terhadap tata kelola keamanan teknologi informasi perpustakaan yang berjalan dan menghasilkan model referensi tata kelola keamanan informasi di Dinas perpustakaan dan Arsip Daerah Kota Bandung. Analisis yang dilakukan dengan alat bantu pengukuran tata kelola keamanan informasi meliputi penurunan tujuan organisasi dan TI, pemetaan proses tata kelola terhadap proses mengacu pada COBIT 5, pemodelan referensi proses pemodelan penilaian proses, analisis *Capability Level*, Hasil analisis yang ada diharapkan dapat membantu dalam menemukan formulasi yang tepat untuk mengukur tata kelola yang ada di organisasi. Penerapan tata kelola keamanan informasi yang direkomendasikan merujuk kepada pendekatan manajemen perubahan dengan pendekatan diadopsi oleh COBIT 5 Implementation menjadi tujuh fase dalam siklus. Setiap fase tersebut terdiri dari tiga lapisan siklus yaitu Manajemen Program, Pemberdayaan Perubahan dan Siklus Perbaikan yang berkelanjutan, untuk peningkatan pengelolaan tata kelola keamanan informasi.

Kata kunci—COBIT 5; penilaian, tata kelola keamanan informasi; teknologi informasi perpustakaan; Dispusip.

I. PENDAHULUAN

Penilaian pada tata kelola keamanan informasi sering digunakan untuk menyelesaikan langkah awal untuk mengembangkan rencana strategis IT. Dinas Perpustakaan dan Arsip Daerah Kota Bandung (Dispusip) saat ini dalam menjalankan Sistem informasi perpustakaan belum menggunakan prosedur kerja tata kelola keamanan informasi yang baik. Sistem informasi perpustakaan. merupakan strategi yang sangat tepat untuk agar dapat meningkatkan pelayanannya terhadap masyarakat. Memanfaatkan Sistem Informasi Perpustakaan dalam tiga tingkatan yaitu memberikan dukungan untuk pelayanan Perpustakaan, sebagai alat bantu pengelolaan perpustakaan dan sarana komunikasi serta pemanfaatan teknologi informasi untuk membantu pengambilan keputusan.

Namun pelaksanaan Tata Kelola Sistem Keamanan Informasi di Dispusip masih belum optimal. Hal ini terlihat dari belum terdapatnya kebijakan mengenai TI dan sistem keamanan informasi seperti manajemen pengguna, manajemen keamanan, manajemen *backup* sistem, integrasi pengelolaan data, strategi penanggulangan bencana (*disaster recovery*). penanganan Risk IT, pemisahan jaringan dan tanggung jawab pihak ketiga dan belum adanya personil *Security Engineer* atau *Information Security* yang khusus menangani keamanan sistem. Untuk itu diperlukan suatu penilaian tata kelola teknologi informasi terkait pengelolaan keamanan sistem sehingga semua risiko yang teridentifikasi dapat dicegah sekaligus mengoptimalkan kinerja teknologi informasi agar lebih mempunyai nilai tambah bagi proses bisnis yang dijalankan, di samping itu diperlukan juga suatu mekanisme kontrol TI untuk memberikan umpan balik terhadap kebijakan atau prosedur keamanan. Panduan Tata kelola TI yang digunakan kerangka kerja *COBIT (Control Objective for Information and Related Technology*) yang dipublikasikan oleh ISACA. Merupakan standar yang diakui secara internasional karena memiliki cara yang baik di bidang keamanan.

II. METODE

A. Rancangan Penelitian

Kerangka penelitian yang dilakukan menggunakan metode kualitatif karena objek penelitiannya bersifat alamiah. Metode penelitian kualitatif digunakan untuk meneliti suatu objek yang alamiah yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari objek penelitian yang diamati.

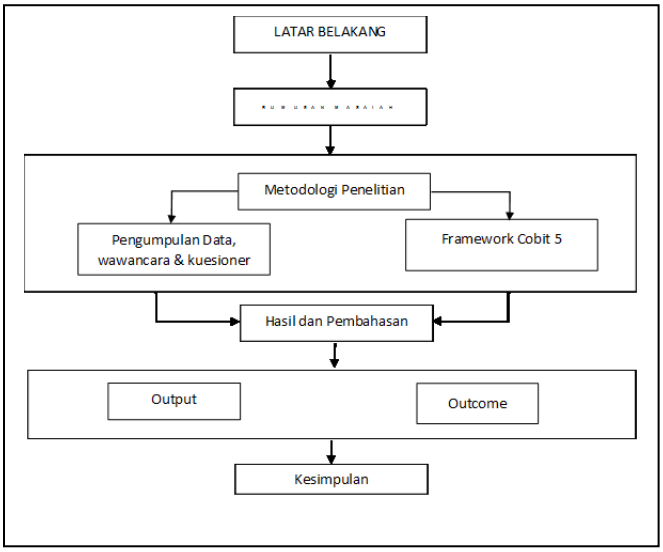
B. Sasaran Penelitian

Populasi dalam penelitian ini adalah pegawai yang ada di Dinas Perpustakaan dan Arsip Daerah Kota Bandung. Namun karena unit analisis tersebut jumlahnya kurang dari 100, untuk menjaga validitas dan reliabilitas pengukuran maka dalam penelitian ini seluruh anggota populasi dijadikan sebagai responden. Dengan demikian sensus dalam penelitian ini adalah (N) 10 orang.

ISBN: 978-602-50525-0-7

C. *Metode Pengumpulan Data*

Populasi dalam penelitian ini adalah pegawai yang ada di Dinas Perpustakaan dan Arsip Daerah Kota Bandung. Namun karena unit analisis tersebut jumlahnya kurang dari 100, untuk menjaga validitas dan reliabilitas pengukuran maka dalam penelitian ini seluruh anggota populasi dijadikan sebagai responden. Dengan demikian sensus dalam penelitian ini adalah (N) 10 orang. Kerangka penelitian dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Penelitian

D. *COBIT – Control Objectives for Information and related Technology*

COBIT Framework dikembangkan oleh *IT Governance Institute*, sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat.

COBIT Framework terdiri atas 2 domain utama:

- *Governance of Enterprise IT* (GEIT)
- *Management of Enterprise IT*

E. *Prinsip dalam COBIT 5*

COBIT 5 dibangun di atas 5 prinsip utama untuk tata kelola dan manajemen teknologi informasi perusahaan. Pemaparan mengenai prinsip-prinsip COBIT 5 :

a. Memenuhi Kebutuhan Pemangku Kepentingan *(Meeting Stakeholder Needs)*.
b. Mencakup Sampai Proses Akhir Suatu Organisasi/Organisasi (*Covering the Enterprise End to End*).
c. Menggunakan Satu Kerangka Kerja Terintegrasi (*Applying a Single Integrated Framework*).
d. Melakukan Pendekatan Secara Menyeluruh (*Enabling a Holistic Approach*).

F. *Metode Analisis Data*

Pemilihan domain COBIT didapatkan dengan menyelaraskan tujuan bisnis dengan tujuan IT. Penelitian difokuskan pada salah satu visi dan misi IT pada Dispusip, yang berkaitan dengan visi dan misi Dispusip. Visi dan misi IT Dispusip yaitu kelancaran proses bisnis yang diwujudkan dengan meminimalisir *down time company* dengan adanya infrastruktur yang berjalan dengan baik.

Metode yang digunakan COBiT 5 menentukan strategi, konsep dan proses yang terkait dengan Manajemen IT, COBiT juga digunakan untuk mengevaluasi faktor penentu keberhasilan, metrik, indikator dan audit. Tahapan-tahapan analisis diawali dengan wawancara untuk mengetahui tingkat kematangan yang diharapkan ke depan sehingga akan diketahui gap di antara kematangan yang diharapkan. Berdasarkan hasil pengukuran tersebut akan diidentifikasi tujuan organisasi (*enterprise goals*/EG) dan tujuan terkait TI (IT-*related goals*/ITRG) yang bersifat generik berdasarkan dimensi *balance scorecard* (BSC) berdasarkan COBiT yang dapat memberikan saran dan rekomendasi di perusahaan, lihat pada Tabel 1.

TABEL 1. TUJUAN IT

Tujuan Perusahaan	**Tujuan IT**			
	EG-02	EG-06	EG-11	EG-14
ITRG-01	P	P	P	S
ITRG-04	P	P	P	S
ITRG-07	P	P	P	S
ITRG-08	S	S	P	S
ITRG-09	S	S	P	P
ITRG-10	P	P	P	S
ITRG-12	S	S	P	S
ITRG-14	S	S	P	S

III. HASIL DAN DISKUSI

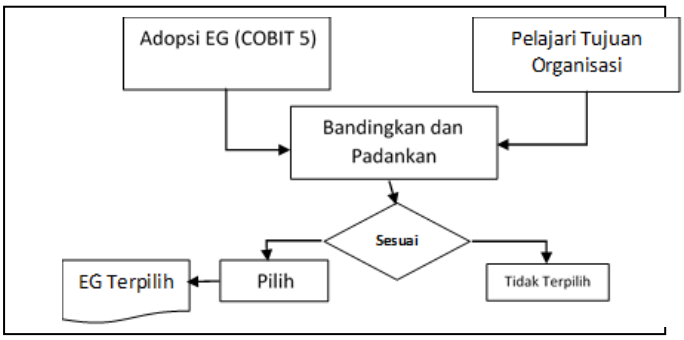
Dinas Perpustakaan dan Arsip Daerah Kota Bandung menerapkan teknologi informasi sebagai penunjang tercapainya tujuan organisasi dan membantu perpustakaan dalam efisiensi proses bisnis perpustakaan. Teknologi informasi yang diterapkan perpustakaan:

1. Aplikasi Inlis Lite (Integrated Library System)
2. Modul *back office*
3. Modul Online Public Access Catalogue (OPAC)
4. Modul keanggotaan online.
5. SMS *Gateway* Perpustakaan
6. Aplikasi Statistik Pengunjung
7. Infrastruktur Server.
8. Web Dispusip.http://dispusip.bandung.go.id

A. *Analisis Kebutuhan*

Pada tahap ini menjelaskan tentang posisi organisasi saat ini yang berhubungan dengan TI. Manajemen perlu mengetahui kemampuan saat ini dan kekurangan organisasi. Hal ini dicapai dengan penilaian kemampuan proses terhadap status proses yang dipilih. Penilaian yang dilakukan pada bagian ini dengan alat bantu pengukuran tata kelola keamanan informasi meliputi penurunan tujuan organisasi dan TI, pemetaan proses tata kelola terhadap proses manajemen layanan, pemodelan referensi proses, dan pemodelan penilaian proses. Hasil penilaian yang ada diharapkan dapat membantu dalam menemukan formula yang tepat untuk mengukur tata kelola yang ada di organisasi, lihat Gambar 2 dan Tabel 2.

ISBN: 978-602-50525-0-7



Gambar 2. Alur Pemetaan Sumber : Penyusunan Proses Tata Kelola Keamanan Informasi dan Manajemen layanan TI berbasis COBIT 5 (Perdana Kusuma MT dan Aries Syamsuddin, 2014)

TABEL 2. TUJUAN ORGANISASI

BSC	EG	Y/T	Tujuan Organisasi	Indikator Kinerja Utama
Financial	EG-02	Y	Meningkatkan minta Baca Masyarakat	Meningkatkan jumlah pemustaka Meningkatkan jumlah koleksi bahan pustaka Meningkatkan jumlah perpustakaan wilayah terbina
Customer	EG-06	Y	Meningkatkan penyelenggaraan kearsipan	Meningkatkan jumlah koleksi bahan pustaka Meningkatkan jumlah SKPD yang menerapkan pengelolaan arsip secara baku
			Meningkatkan pelayanan kepada masyarakat	Terwujudnya peningkatan kualitas pelayanan publik
Internal Bisnis Proses	EG-011	Y	Meningkatkan pelayanan kepada masyarakat	Terwujudnya peningkatan kualitas pelayanan publik
	EG-014	Y	Terwujudnya Kinerja yang akuntabel	Meningkatnya kapasitas dan akuntabilitas kinerja birokrasi
			Meningkatkan penyelenggaraan kearsipan	Meningkatnya SDM Pengelolaan Kearsipan

B. *Analisis Pemetaan Tujuan IT*

Pemetaan tujuan IT merupakan turunan dari tujuan organisasi yang digunakan untuk menentukan lingkup keamanan informasi yang lebih spesifik pada IT. Pemetaan ini bertujuan untuk menurunkan dan merumuskan tujuan IT ke dalam bentuk ITRG yang bersifat generik. Skema pemetaan antara tujuan generik IT dan untuk menghasilkan proses tata kelola yang terpilih dalam penentuan lingkup Tata Kelola Keamanan Informasi berdasarkan tujuan organisasi dan TI.

C. *Pemetaan Tujuan TI dan Proses Tata Kelola*

Rangkuman proses tata kelola terpilih diperlihatkan pada Tabel 3.

TABEL 3. RANGKUMAN TUJUAN TI DAN PROSES TATA KELOLA

ID	Nama Proses Tata Kelola (Domain)	P/S	Y/N
APO13	Manager Security	P	Y
DSS05	Manage Security Services	P	Y

Pemetaan IT *Goal* dengan Proses CobIT 5 diperlihatkan pada Tabel 4.

TABEL 4. PEMETAAN IT GOAL DAN PROSES COBIT 5

ID	Nama Proses Tata Kelola (Domain)	ITRG-10 Keamanan informasi, infrastruktur pengolahan dan aplikasi
APO13	Manager Security	P
DSS05	Manage Security Services	P

D. *Diagram RACI*

Diagram RACI merupakan gambaran peran dari pemangku kepentingan diperlihatkan pada Tabel 5.

TABEL 5. TABEL DIAGRAM RACI

No	Key Management Practice	Kepala Dispusip	Sub Bag Tata Usaha	KaSi Pengelolaan Perpustakaan	KaSi Pengelolaan Kearsipan	KaSi bina Perpustakaan dan Kearsipan	Fungsional Perpustakaan	Staff Sub Bag Tata USaha	Staff SubBag Peprutakaan	Staff Sub Bag Kearsipan	Staff Sub Bag bian Perpus
1	**APO-13 Manajemen Keamanan**	**C**	**C**	**R**	**R**	**I**	**I**	**C**	**R**	**R**	**I**
	APO13-01	*	*	*	*	*					
	APO13-02	*	*	*	*	*					
	APO13-03		*	*	*	*					
2	**DSS-05 Manajemen Layanan Keamanan**						**I**	**C**	**R**	**R**	**I**
	DSS05-01						*	*	*	*	*
	DSS05-02						*	*	*	*	*
	DSS05-03						*	*	*	*	*
	DSS05-04						*	*	*	*	*
	DSS05-05						*	*	*	*	*
	DSS05-06						*	*	*	*	*
	DSS05-07						*	*	*	*	*

E. *Hasil Model Penilaian Proses*

Penilaian model penilaian proses bertujuan untuk membuat model penilaian proses tata kelola keamanan informasi berdasarkan level pencapaian kemampuan. Model ini dijadikan sebagai dasar perhitungan analisis kesenjangan pada proses tata kelola keamanan informasi. Komponen proses yang dinilai (meliputi: aktivitas, keluaran, GP, GWP dan GR) memiliki rentang nilai:

1) Tidak ada, artinya komponen proses yang dimaksud tidak ada atau tidak dilakukan,

ISBN: 978-602-50525-0-7

2) Sebagian kecil, artinya telah ada sedikit bukti adanya atau dilaksanakannya komponen proses yang dimaksud,
3) Sebagian besar, artinya telah banyak bukti adanya atau dilaksanakannya komponen proses yang dimaksud,
4) Penuh, artinya komponen proses yang dimaksud telah ada atau dilaksanakan secara maksimal. Pengolahan penilaian proses dapat dilihat pada Tabel 6.

TABEL 6. PENGOLAHAN PENILAIAN PROSES

Proses	Responden	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Capability level (%)
APO13-01	5	4.48	0.42	0	0	0	0	20.0
APO13-02	5	4.62	0.28	0	0	0	0	20.0
APO13-03	4	3.8	0.2	0	0	0	0	25.0
DSS05-01	3	2.38	0.68	0	0	0	0	33.3
DSS05-02	3	0.99	1.98	0	0	0	0	33.3
DSS05-03	3	1.21	1.98	0	0	0	0	33.3
DSS05-04	3	1.26	1.68	0	0	0	0	33.3
DSS05-05	3	0.42	2.52	0	0	0	0	33.3
DSS05-06	3	2.8	0.2	0	0	0	0	33.3
DSS05-07	3	2.2	0.8	0	0	0	0	33.3

Model penilaian proses merupakan suatu model yang digunakan untuk menilai kemampuan proses tata kelola berdasarkan suatu model referensi proses. Model penilaian proses menggunakan sumber data terakhir.

1) Model referensi proses yang dijadikan sebagai dasar penilaian kemampuan dimensi proses pada level 1
2) ISO/IEC 15504 *series* yang dijadikan dasar penentuan level atau dimensi *practices, generic work products* dan *generic resource*.
3) COBIT 5 *for Information Security* yang digunakan untuk mendefinisikan aktivitas dari setiap *base practice*.
4) COBIT 5 *Process Assessment* Model yang digunakan untuk mendefinisikan *generic practices* dan *generic work products model* penilaian proses tata kelola keamanan informasi terdiri atas dua bagian yaitu komponen rekapitulasi dan komponen rincian proses. Model penilaian proses APO13 dapat dilihap pada Tabel 7.

TABEL 7. MODEL PENILAIAN PROSES APO13

	SUMMARY									
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1,1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA	PA 5.1	PA 5.2
Target	F	F	L	L						
Rating	F	F	P	P						
Rating by criteria	F	F	P	P						
Capability Level Achieved	P	P	P	P						

F. Analisis Kesenjangan

Analisis kesenjangan merupakan proses yang bertujuan untuk mengetahui kondisi *capability*/kematangan tata kelola keamanan informasi yang ada saat ini dan harapan yang akan dicapai oleh suatu organisasi, model penilaian proses DSS05 dapat dilihat pada tabel 8.

TABEL 8. MODEL PENILAIAN PROSES DSS05

	SUMMARY									
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 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
Target	F	F	L	L						
Rating	F	F	P	P						
Rating by criteria	F	F	P	P						
Capability Level Achieved	P	P	P	P						

G. Rekomendasi

Rekomendasi tata kelola keamanan informasi dilakukan bertujuan untuk membantu organisasi dalam mengelola dan mengamankan informasi yang dianggap sebagai sumber daya yang penting. Rekomendasi juga dilakukan untuk perbaikan yang di usulkan untuk objek penelitian di Kapusarda. Dari Rencana Strategis (restra) Kapusarda Kota Bandung dipetakan terhadap tujuan perusahaan (*Enterprose Goal*) COBIT 5. Setelah didapatkan tujuan perusahaan maka tujuan perusahaan tersebut dipetakan terhadap Tujuan Terkait (*IT Related Goa*l) COBIT 5. Tujuan Terkait TI hasil pemetaan juga dipetakan terhadap domain COBIT 5 untuk mendapat keamanan Informasi (*For Information Security*). Ada dua kategori yaitu primer dan sekunder yang bisa dipilih dengan memfokuskan pada kategori primer. Proses hasil pemetaan ini yang nantinya akan menjadi acuan.

Tingkat kemampuan saat ini mengarah pada level 1 yaitu proses yang sudah diterapkan, namun belum sepenuhnya

mencapai tujuan yang diharapkan. Tingkat kemampuan yang diharapkan adalah level 1 harus memiliki *Best Practices* dan *Work Product* yang ada pada COBIT 5. Pencapaian level 1 keluaran(*output*) *work product* APO13 dan pencapaian leve 1 keluaran(*output) work produt DSS05* terdapat pada Tabel 9 dan Tabel 10.

TABEL 9. PENCAPAIAN LEVEL 1 OUTPUT WORK PRODUCT APO13

Domain	**Deskripsi Output Work Product**	**Cakupan Dokumen rekomendasi**	**Nama Kebijakan/ Prosedur**
APO13-01 WP-1, WP-2	• Pernyataan lingkup SMKI (Sistem Manajemen Keamanan Informasi) • Kebijakan SMKI	Kebijakan Keamanan Informasi Menyatakan komitmen manajemen / pimpinan instansi / lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan tujuan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggung jawab keamanan informasi	Kebijakan
APO13-02 WP-3	• Business case keamanan informasi	Manajemen Kelangsungan Usaha (*Business Continuity Management*) Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana / k darurat. Dokumen ini juga memuat tim yang bertanggung jawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	Kebijakan
APO13-03 WP-4, WP-5	• Rekomendasi untuk perbaikan SMKI • Laporan audit SMKI	Audit Internal SMKI Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor.	Prosedur

TABEL 10. PENCAPAIAN LEVEL 1 OUTPUT WORK PRODUCT DSS05

Domain	Deskripsi Output Work Product	Cakupan Dokumen Rekomendasi	Nama Kebijakan/ Prosedur
DSS05-01 WP-1, WP-2	• Kebijakan pencegahan perangkat lunak berbahaya • Evaluasi ancaman yang potensial	Pengendalian Instalasi *Software* & Hak Kekayaan Intelektual Berisi daftar *software* standar yang diizinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan *software* yang tidak diizinkan.	Prosedur
DSS05-02 WP-3	• Kebijakan keamanan koneksi • Hasil *penetration test*	Pemantauan (*Monitoring*) Penggunaan Fasilitas TIK Berisi proses pemantauan penggunaan CPU, *storage*, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil pemantauan.	Prosedur
DSS05-03 WP-4,WP-5	• Kebijakan keamanan pada perangkat *endpoint*	Tindakan Perbaikan & Pencegahan Berisi tata cara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TIK.	Prosedur
DSS05-04	• Hasil kajian akun pengguna dan hak aksesnya • Hak akses pengguna yang disetujui	Kebijakan Pengamanan Akses Fisik dan Lojik	Kebijakan
DSS05-05	• *Access logs* • Permintaan akses yang disetujui	*User Access Management* Berisi proses dan tata cara pendaftaran, penghapusan dan peninjauan hak akses *user*, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, *database*, internet, email dan internet).	Prosedur
DSS05.06	• Hak akses khusus • Penyimpan dokumen sensitif dan perangkatnya	Pengendalian Dokumen Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan dokumen jika tidak digunakan dan daftar serta pengendalian dokumen eksternal yang menjadi rujukan.	Prosedur
DSS05.07	• Tiket insiden keamanan • Karakteristik insiden keamanan • Log kejadian keamanan	Pengelolaan & Pelaporan Insiden Keamanan Informasi Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan dan pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	Prosedur

IV. KESIMPULAN

Hasil Penelitian skala *rating* kapabilitas APO13 dan DSS05 berada di level P (Partially Achieved) yang berarti ada beberapa bukti dari aktivitas yang dijalankan dan beberapa pencapaian atribut yang didefinisikan dalam penilaian proses. Sedangkan level *capability* berada di level 1 (performed process) yang artinya ada proses dilaksanakan namun pencapaian tiap prosesnya belum terpenuhi semuanya dan belum mencapai tujuan proses yang diharapkan Dispusip. Hasil analisis penelitian menemukan gap pada sub domain APO13 dan DSS05 hanya mampu memperoleh nilai rata-rata 1.0.

Langkah penerapan tata kelola keamanan informasi yang direkomendasikan merujuk kepada pendekatan manajemen perubahan dengan pendekatan diadopsi oleh COBIT 5. Rekomendasi yang diberikan yaitu mengusulkan langkah pencapaian untuk memperoleh level 1 *output work product* APO13 dan DSS05 dan kebijakan beserta panduan hasil analisis kesenjangan.

Kebijakan Informasi yang diadopsi dari ISO 27001 terdiri dari 3 kebijakan, 7 prosedur. Dokumen kebijakan keamanan informasi disetujui oleh manajemen puncak.

Terdapat beberapa saran untuk peningkatan pencapaian tata kelola keamanan informasi, yaitu:

1) Langkah pertama yang harus dilakukan oleh Dispusip dalam memperbaiki Tata kelola keamanan informasi pada layanan tata kelola sistem perpustakaan yang tepat untuk diterapkan pada organisasi adalah meningkatkan tata kelola pada sub domain APO13 dan DSS05 sesuai rekomendasi yang diberikan penulis.
2) Evaluasi tata kelola teknologi keamanan pada Dinas perpustakaan dan arsip daerah masa mendatang dapat menggunakan model COBIT5 dan panduan yang mengadopsi ISO 27001

DAFTAR PUSTAKA

[1] D. Ciptaningrum, E. Nugroho, D. Adhipta,, "Pemetaan Tujuan Kaskade Cobit 5 Dalam Perumusan Proses Audit Keamanan Sistem Informasi Di Pemerintahan Kota Yogyakarta," *Seminar Nasional Teknologi Informasi dan Multimedia STMIK AMIKOM Yogyakarta.,* 2015, Februari 6-8.

[2] Direktorat Keamanan Informasi, Tim, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.Direktorat Keamanan Informasi", Direktorat Jenderal Aplikasi Informatika, Kementrian Komunikasi dan Informatika RI, 2011'

[3] D. Firmansyah, "Pengukuran Kapabilitas Pengelolaan Sistem Informasi *Sub Domain Deliver, Service, Support* 01 Menggunakan Framework Cobit 5". (Studi Kasus : Politeknik Komputer Niaga LPKIA Bandung). 2015.

[4] ISACA,"COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*"*. USA: *IT Governance Institut"*.2012

[5] ISACA. "COBIT 5 Enabling Processes*."* USA: *IT Governance Institute*. 2012

[6] ISACA. "COBIT 5 Implementation. USA": IT Governance Institute.2012

[7] ISACA. "COBIT 5 Process Assessment Model. USA": IT Governance Institute.2013

[8] ISACA. "COBIT 5 Process Reference Guide Exposure Draft. USA": IT Governance Institute.2011

[9] ISO 13000. "International Organization for Standardization (ISO). Risk Management: Principles and Guidelines." (http://www.iso.org/iso/home/standards/iso31000.htm).2009

[10] A. Kadir. " Pengenalan Sistem Informasi". Yoyakarta: Andi Offest 2003.

[11] P. Kusumah, A. Syamsudin "Penyusunan Proses Tata Kelola Keamanan Informasi dan Manajemen Layanan IT Berbasis COBIT 5".2014

[12] Kapusarda., Rencana Strategis (RENSTRA) Kantor Pusarda Kota Bandung tahun 2013-2018".2013

[13] Kapusarda.".,Laporan Kinerja Instansi Pemerintah LKIP tahun 2014".2014

[14] Manstan, Adrian, Ignatius, SNATI, 2015

[15] M.Gehrmann," Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology, for Management in Organissation", 2012,

[16] M. I., Putri, "Tata Kelola Informasi (IT Governance) Menggunakan Framework Cobit 5 (Studi kasus Dewan Kehormatan Penyelenggaran Pemilu)", Program Studi Sistem Informasi, Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.,2014

[17] F. Purwaningtyas, "Aset Informasi Perpustakaan (Tata Kelola dan Keamanan)", Majalah Online Edisi Vol 16 No 2, Perpustakaan Nasional Republik Indonesia, Indonesi Gemar membaca.

[18] http://dev.perpusnas.go.id/magazine/aset-informasi-perpustakaan-tata-kelolakeamanan/ . 2014, Agustus

[19] Tulus, Purnomo, Ariana , ISO 31000

[20] http://blogs.itb.ac.id/2321511arianael5216mrkisem1t15d16mr/2015/iso31000/

[21] I. N. S. Saputra, "Pengukuran Tingkat Kapabilitas dan Perbaikan Tata Kelola Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 dan ITIL V3 2011 (Studi Kasus PT XYZ)". Fakultas Ilmu Komputer, Program Studi Magister Teknologi Informasi Jakarta. 2013

[22] S. W. Sembiring, "Evaluasi Penerapan Teknologi Informasi menggunakan Model COBIT Framework 4.1 (Studi Kasus : PT Prudential Indonesia)", Program Studi Magister Teknik Informatika Program Pascasarjana Universitas Atmajaya Yogyakarta, 2013.