TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS PADA DINAS KOMUNIKASI DAN INFORMASI KOTA SUKABUMI)

Lelah[1)], Toto Suharto[2)]
Universitas Muhammadiyah Sukabumi[1)], Universitas Langlangbuana Bandung[2)]
Email : lelah@ummi.ac.id, tsuharto@gmail.com

Abstract

DISKOMINFO Sukabumi city is Office that has the task of implementing regional authority in field of management of Information and Communication Technology. The consequence of application of Information and Communication Technology (ICT) is with emergence of security risks. As happened in Sukabumi City Government Information System, hacking occurs by unauthorized parties. There are several ways to maintain information security, by applying information security to information technology layer technically or by doing governance. The implementation of this governance is a necessity and has become a necessity and a demand. One of them is using COBIT 5 framework with the COBIT for information security section, which focuses on information security and provides more complete guidelines and practices for information security professionals and other related parties at each interprise level. In a study at DISKOMINFO Kota Sukabumi, the selection of the COBIT 5 framework domain, was taken by mapping the organization's objectives with EG COBIT and ITRG goals. From the election was taken the enabler of EDM01, APO01, APO02, APO03, BAI02, DSS03, DSS05. The results show that Information Technology security management in DISKOMINFO is still at level 1.

Keywords : DISKOMINFO, COBIT 5, Information Technology Security Governance

Pendahuluan

Latar Belakang

Dinas Komunikasi dan Informatika atau DISKOMINFO menjadi salah satu lembaga yang berada di pemerintahan yang mengelola Teknologi Informasi Dan Komunikasi (TIK). Salah satunya DISKOMINFO Kota Sukabumi. Berdasarkan Peraturan Walikota tentang kedudukan, Susunan Organisasi, Tugas Pokok, Fungsi dan Tata Kerja Dinas Komunikasi dan Informatika, Dinas Komunikasi dan Informatika adalah Dinas yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan Informatika, urusan pemerintahan bidang Statistik dan urusan pemerintahan bidang Persandian. (Peraturan Walikota Sukabumi Nomor 44 Tahun 2016).

Berdasarkan tugas pokok dan fungsi yang besar dalam membangun Teknologi Informasi dan Komunikasi (TIK), dan Kota Sukabumi sebagai *smartcity*, dimana *smartcity* tersebut merupakan salah satu tujuan Pemerintah Kota Sukabumi sebagai upaya untuk mempermudah pelayanan kepada masyarakat. Pada implementasi *smartcity*, dimana aplikasi digital memegang peran penting. Aplikasi-aplikasi ini akan berfokus pada berbagai bidang, misalnya permasalahan bisnis hingga pemetaan untuk memudahkan aksi cepat tanggap di masyarakat. Untuk itu semua aplikasi yang ada di setiap SKPD dan BUMD harus terintegrasi dengan aplikasi yang ada di Pemda Kota Sukabumi, dengan demikian pengelolaan aplikasi di Pemda Kota Sukabumi menjadi tanggung jawab DISKOMINFO, untuk itu keputusan Teknologi Informasi dan Komunikasi harus terencana dengan baik karena Teknologi Informasi dan Komunikasi (TIK) merupakan pendorong utama proses transformasi bisnis yang memberi imbas penting bagi organisasi dalam pencapaian misi, visi dan tujuan strategik.

Konsekuensi dari penerapan Teknologi Informasi dan Komunikasi (TIK) adalah dengan munculnya resiko keamanan. Pada tahun 2016 IDSIRTII melakukan stastistik tren serangan internet terhadap *domain* .go.id. maka, terlihat bahwa serangan paling banyak dilakukan oleh *web defaceman*, disusul *malware, fishing, spam, bruto forse*, dan *IPR*. Hal ini memperkuat bahwa instansi Pemerintahan harus mengamankan asetnya. Semakin berkembang ilmu pengetahuan dan teknologi maka makin banyak juga celah keamanan, yang akan mengancam keberlangsungan proses bisnis suatu organisasi. Lemahnya sistem keamanan informasi dapat menimbulkan efek yang luas terhadap keberlangsungan organisasi. Seperti yang terjadi pada Sistem Informasi Pemerintahan Kota Sukabumi, terjadi peretasan oleh pihak yang tidak berkepentingan (www.techno.or.id).

Ada beberapa cara untuk menjaga keamanan informasi, diantaranya dengan menerapkan keamanan informasi pada lapisan teknologi informasi secara teknis atau dengan melakukan tata kelola. Informasi itu sendiri merupakan aset yang sangat berharga bagi sebuah organisasi karena salah satu sumber strategis dalam meningkatkan nilai usaha. Oleh karena itu perlu dilakukannya perlindungan terhadap keamanan informasi tersebut, karena keamanan informasi itu sendiri bagian integral dari tata kelola organisasi, dan tujuan dari pengamanan itu sendiri adalah untuk meyakinkan integritas, kelanjutan dan kerahasiaan dari pengolahan data. Seperti tercantum dalam Permen Kominfo No 4 tahun 2016 tentang sistem pengamanan teknologi informasi. Kemanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses dan aktivitas untuk melindungi informasi dari berbagai ancaman, yang akan menyebabkan kerugian bagi kelangsungan hidup organisasi akan tetapi untuk pengamanan secara menyeluruh maka perlu adanya penerapan tata kelola teknologi informasi dan komunikasi (TIK). Hal ini sudah diatur dalam Permen Kominfo Nomor : 41/PER/MEN.KOMINFO/11/2017. Selain itu faktor pendorong perlunya dibuat tata kelola pada DISKOMINFO Kota Sukabumi adalah adanya tanggung jawab terhadap pengamanan teknologi informasi pada lingkungan PEMDA Kota Sukabumi, penerapan IT dengan investasi yang besar, dan adanya program Sukabumi *smartcity*, karena pengamanan yang dilakukan harus secara menyeluruh.

Agar dapat mengetahui sejauh mana tatakelola keamanan informasi yang baik dan benar, terdapat beberapa model, model tersebut haruslah berdasarkan standar yang umum dan diakui secara luas. di antaranya adalah *ITIL* (*The IT Infrastructure Library*), *Control Objectives for Information and related Technology* (*COBIT*), ISO/IEC 27001, COSO dll. Dengan menggunakan standar-standar tersebut, maka tujuan penerapan TI di sebuah perusahaan akan sesuai dengan tujuan yang diharapkan dan menghindarkan dari terjadinya kerugian akibat risiko-risiko penerapan yang tidak terpetakan. Dari keempat model tata kelola TI yang ada dipilihlah COBIT. *COBIT* memiliki kedetailan atau kedalaman standar dalam hal teknis dan operasional serta kelengkapan proses TI yang baik. Selian itu *COBIT* merupakan model yang paling lengkap untuk menjadi acuan dalam membuat tata kelola teknologi informasi, karena semua proses pada setiap *framework* akan terwakili. Selain itu juga, dari penelitian-penelitian sebelumnya *COBIT* termasuk *framework* tata kelola teknologi informasi yang ditujukan untuk *enterprise (*Perusahaan). *(Overview Of International IT Guidance : 2008).* Dalam hal ini DISKOMINFO dapat digolongkan sebagai organisasi publik atau sebuah *enterprise*. Seperti dalam jurnal Sofian Lusa dan Dana Indra Sensuse yang berjudul Kajian Perkembangan Usulan Perancangan *Enterprise Architecture Framework* pada tahun 2011, di sana dijelaskan bahwa *enterprise* sebagai organisasi publik, yaitu organisasi yang mewadahi seluruh lapisan masyarakat dengan lingkup negara yang memiliki kewenangan yang sah dibidang politik, administrasi pemerintahan, dan hukum secara terlembaga.

Pada seri *COBIT 5* terdapat bagian *COBIT for information security*, dimana berfokus pada keamanan informasi dan menyediakan pedoman lebih lengkap dan praktik untuk para profesional keamanan informasi dan pihak lain yang terkait pada setiap *level interprise.*

Rumusan Masalah

Berikut ini adalah rumusan masalah dari penelitian ini, sebagai berikut:

1. Bagaimana menyertakan Keamanan teknologi Informasi pada Tata kelola ?
2. Bagaimana melakukan proses pemilihan dari tujuan organisasi sampai proses terpilih, dengan membandingkan tujuan organisasi dengan Enterprise Goal COBIT 5 dan IT Relation Goal ?
3. Bagaimana cara melakukan penilaian terhadap tingkat kematangan TI dengan *COBIT Process Assessment Model* pada DISKOMINFO Kota Sukabumi ?
4. Rekomendasi apa yang dihasilkan untuk DISKOMINFO Kota Sukabumi agar penerapan tata kelola keamanan informasi sesuai dengan harapan?

Batasan Masalah

Adapun batasan permasalahan pada penelitian ini adalah:

1. Ruang lingkup kebutuhan meliputi tujuan organisasi, tujuan TI, tujuan kemanan TI dan proses layanan pada DISKOMINFO Kota Sukabumi.
2. Penelitian ini dilakukan dengan menggunakan *COBIT* 5 pada bagian *COBIT 5 for information and Security*, untuk seluruh domain COBIT 5.

Maksud dan Tujuan

Maksud penelitian ini adalah untuk membuat *template* tata kelola keamanan informasi pada DISKOMINFO Kota Sukabumi menggunakan COBIT 5.
Sedangkan Tujuan dari penelitian tesis ini adalah:

1. Untuk mengetahui pengelolaan IT di DISKOMINFO Kota Sukabumi.
2. Untuk mengetahui framework *COBIT for Information security.*
3. Untuk mengetahui bagaimana cara menyertakan keamanan pada Tata Kelola
4. Untuk mengetahui tingkat kematangan TI dengan *COBIT Process Assessment Model* pada DISKOMINFO Kota Sukabumi.
5. Untuk mengetahui rekomendasi apa yang dihasilkan dari proses penilaian pada DISKOMINFO Kota Sukabumi agar penerapan tata kelola keamanan informasi sesuai dengan harapan.

Manfaat Penelitian

Manfaat dari penelitian ini diantaranya:

1. Menganalisa pengelolaan TI yang ada pada DISKOMINFO Kota Sukabumi.
2. Menjadi satu informasi untuk merancang Tata Kelola TI dengan menyertakan unsur keamanan.
3. Dapat menjadi referensi bagi DISKOMINFO Kota Sukabumi dalam membuat tata kelola keamanan informasi sesuai dengan *Framework COBIT 5*.
4. Dapat menjadi referensi bagi penulis lain dalam pembuatan tata kelola keamanan informasi.

Metode Penelitian

Berdasarkan tujuannya, penelitian ini adalah penelitian terapan. Dimana tujuannya menerapkan, menguji dan mengevaluasi kemampuan suatu teori yang diterapkan dalam memecahkan masalah. Pada tesis ini dilakukan penelitian berdasarkan *framework* yang telah ada untuk proses tata kelola keamanan informasi, yaitu menggunakan COBIT 5. Dan akan dilakukan penerapan teori-teori yang ada pada COBIT 5 untuk memecahkan masalah pada pembuatan tata kelola keamaman informasi untuk DISKOMINFO Kota Sukabumi.

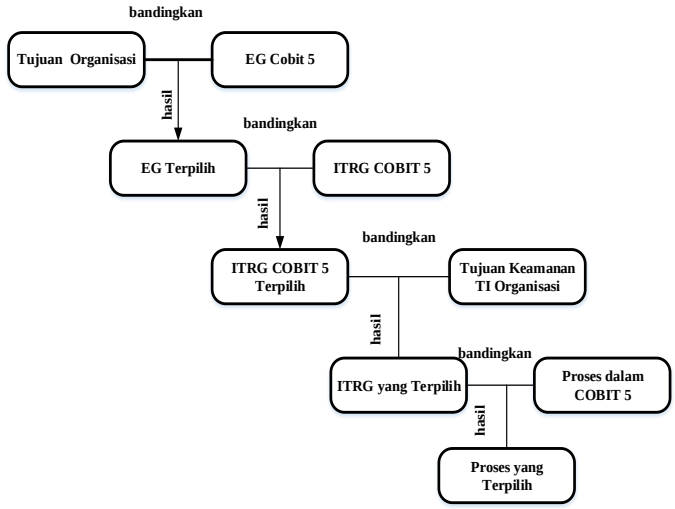
Melihat dari paradigma penelitian dan teknik pengumpulan datanya, maka dalam penelitian ini, termasuk kedalam penelitian *kualitatif* dan *kuantitatif.* Data *kualitatif* yang penulis perlukan dalam penelitian ini adalah data visi, misi, tujuan, rencana kerja DISKOMINFO, SOP dan Peraturan perundang-undangan yang mengatur. Dalam penelitian *kuantitatif* ini, penulis memberikan kuesioner atau angket kepada pegawai DISKOMINFO Kota Sukabumi, kemudian dilakukan perhitungan dan uji validitas dan reabilitas.

Hasil Dan Pembahasan

Pada penelitian ini sumber kebutuhan Tata Kelola akan dibatasi pada tujuan organisasi, hal ini diambil sesuai dengan harapan hasil dari tata kelola keamanan informasi dimana sumber keamanan diambil dari tujuan organisasi, yang ditunjang oleh adanya visi, misi dan program kerja.

Penentuan sumber kebutuhan kebutuhan keamanan pada tata kelola keamanan informasi didasarkan pada proses *cascading goals* dari COBIT 5. Dimana tujuan dari *cascading goals* adalah mendapatkan *enablers goals*, yaitu berupa proses yang sesuai

untuk menunjang tujuan organisasi. Pada penelitian ini ditujukan untuk mendapatkan proses yang sesuai untuk pencapaian tujuan DISKOMINFO. Untuk lebih jelasnya, proses *cascading goals* digambarkan dengan lebih rinci pada gambar berikut:



Gambar 1 Proses Pemilihan dari Tujuan Organisasi Sampai Proses Terpilih

Semua enabler proses yang terpilih dlakukan penilaian. Berikut rekapitulasi hasil Pencapaian *Best Practise*

Tabel 1 Rekapitulasi Hasil Pencapaian *Best Practise* Dari Proses Terpilih

No	Enabler Proses	Nilai Pencapaian
1	EDM01	51,27 %
2	APO01	39,15 %
3	APO02	57,42 %
4	APO03	75,57 %
5	BAI02	61,16 %
6	DSS03	38,45 %
7	DSS05	38,41 %

Tabel 2 Rekapitulasi Hasil Pencapaian *Work Products*

No	Enabler Proses	Nilai Pencapaian
1	EDM01	33,33 %
2	APO01	72,73 %
3	APO02	57,14 %
4	APO03	14,28 %
5	BAI02	75,00 %
6	DSS03	50,00 %
7	DSS05	58,33 %

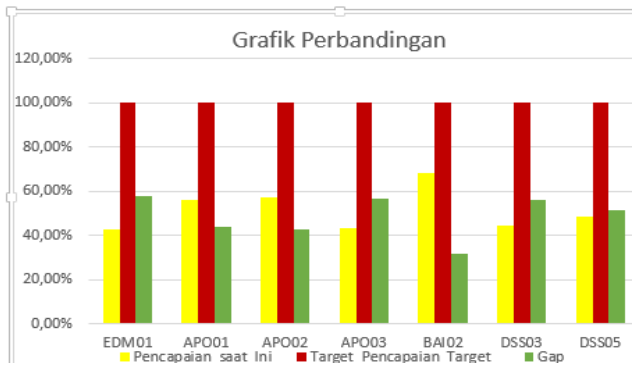
Tabel 3 Rekapitulasi Hasil Penilaian *Best Practise* dan *Work Products*

No	Enabler Proses	*Best Practise*	*Work Products*	Akumulasi	Kriteria pencapaian	Level
1	EDM01	51,27 %	33,33 %	42,51 %	P	0
2	APO01	39,15 %	63,63 %	55,94 %	L	1
3	APO02	57,42 %	42,86 %	57,28 %	L	1
4	APO03	75,57 %	0,00 %	43,42 %	P	0
5	BAI02	61,16 %	25,00 %	68,08 %	L	1
6	DSS03	38,45 %	0,00 %	44,22 %	P	0
7	DSS05	38,41 %	41,67 %	48,37 %	P	0

Berdasarkan data hasil di atas, maka terlihat ada empat proses yang berada pada level 0 dan tiga proses pada level 1. Untuk empat proses belum menunjukkan proses pencapaian karena nilai pencapaian proses kurang dari 50%. Dan tiga proses telah mencapai nilai di antara 50-85%. Hal ini menunjukkan bahwa, perlu adanya pembenahan dan perbaikan untuk tata kelola keamanan TI di DISKOMINFO Kota Sukabumi, supaya dapat mencapai target yang ingin dicapai. Terjadinya perbedaan antara hasil pencapaian sekarang dengan target menimbulkan gap atau pemisah, tujuan akan tercapai jika pemisah tersebut dihilangkan. Berikut digambarkan antara pencapaian nilai kapabilitas saat ini dengan target.

Tabel 4 Perbandingan Pencapaian Nilai dan Target Harapan

No	Enabler Proses	Pencapaian saat Ini	Target Pencapaian Target	Gap
1	EDM01	42,51 %	100 %	57,70 %
2	APO01	55,94 %	100 %	44,06 %
3	APO02	57,28 %	100 %	42,72 %
4	APO03	43,42 %	100 %	56,58 %
5	BAI02	68,08 %	100 %	31,92 %
6	DSS03	44,22 %	100 %	55,78 %
7	DSS05	48,37 %	100 %	51.63 %



Gambar 1 Grafik Perbandingan antara pencapaian saat ini, target dan gap

Target yang ingin dicapai pada pada pembuatan roadamap tata kolola keamanan teknologi informasi saat ini adalah untuk meningkatkan level yang ingin dicapai dari kondisi saat ini. Level kapabilitas saat ini berada pada level 0 dan 1, sedangkan level yang diharapkan adalah level 2 yaitu proses yang diimplementasikan dikelola (direncanakan dan disesuaikan) dan hasilnya ditetapkan, dikontrol dan dipelihara.

Ada dua tahap yang harus dilakukan yaitu :

1. Semua tahap tidak boleh berada pada level 0, dan level 1 harus sudah terpenuhi 100 %.
2. Setelah level 1 terpenuhi, maka level 2, harus terpenuhi minimal 50 % yang terdiri dari dua proses atribut, yaitu *performance management* dan *work products management.*

Dalam rangka mewujudkan peningkatan level kapabilitas tata kelola keamanan teknologi informasi pada DISKOMINFO kota sukabumi yang diinginkan yaitu mencapai level 2, maka tahapan pelaksanaannya adalah :

1. Urutan proses pencapaian dimulai dari urutan proses pada tahapan tata kelola berdasarkan pencapaian masing-masing proses atribut (PA), yaitu dimulai dari pemenuhan proses atribut (PA) 1, kemudian proses atribut (PA) 2.1 dan proses atribut (PA) 2.2 Karena ini akan mendukung implementasi RPJMD Kota Sukabumi, yaitu peningkatan teknologi komunikasi dan informasi, meningkatnya pelayanan masyarakat, didukung penyedian informasi publik secara transparan.
2. Waktu pencapaian tata kelola sampai level 2 ditargetkan selesai pada tahun 2018, hal ini didasarkan pada RPJMD Kota Sukabumi, dimana pengembangan teknologi informasi dan komunikasi menjadi program bagi DISKOMINFO sampai pada tahun 2018.

Adapun sasaran dari tiap tahap pelaksanaannya adalah sebagai berikut :

1. Pada proses atribut (PA)1.1 (*Process Performance),* pada level ini harus mendapatkan nilai F *(fully achieved*) yang artinya bukti pendekatan yang lengkap dan sistematik, pencapaian penuh dan penetapan atribut dalam proses penilaian. Tidak adanya kekurangan yang signifikan terkait atribut dalam proses penilaian. Yaitu persentase pencapaiannya >85-100 % *achievemen*t.
2. Pada proses atribut (PA) 2.1 *Perfeomance Management* mengukur sampai mana kinerja proses dikelola, tabel pengukurannya dapat dilihat pada tabel.. nilai yang ingin dicapai minimal harus L (*Largely achieved)* yaitu >50-85% achievement, yaitu adanya bukti pendekatan sistematik dan pencapaian yang signifikan dan penetapan atribut dalam proses penilaian. Beberapa kelemahan yang terkait dengan atribut dapat muncul dalam proses penilaian.
3. Pada proses atribut (PA) 2.2 *Work Product Management* mengukur sejauh mana hasil kerja yang dihasilkan oleh proses dikelola. Hasil kerja yang dimaksud disini adalah hasil dari proses. nilai yang ingin dicapai minimal harus L (*Largely achieved)* yaitu >50-85% achievement, yaitu adanya bukti pendekatan sistematik dan pencapaian yang signifikan dan penetapan atribut

dalam proses penilaian. Beberapa kelemahan yang terkait dengan atribut dapat muncul dalam proses penilaian.

Indikator pencapaian sasarannya adalah sesuai dengan penjelasan pada setiap level yang process assessment model COBIT 5, yaitu :

1. Proses Atribut 1.1 (*Prosess Performance*)
   Proses meraih tujuan yang sudah ditentukan, dengan memenuhi *Base Practice* dan *Work Product* yang ada.
2. Proses Atribut 2.1 (*Performance Management)*
   a. Objektif performa dari proses teridentifikasi
   b. Performa dari proses direncanakan dan dimonitor.
   c. Performa dari proses disesuaikan untuk memenuhi perencanaan tanggung jawab dan otoritas dari melakukan proses didefinisikan, ditugaskan, dan dikomunikasikan
   d. Sumber daya dan informasi yang dibutuhkan untuk menjalankan proses diidentifikasi, disediakan, dialokasikan dan digunakan
   e. Antarmuka antara pihak yang terlibat dikelola untuk memastikan komunikasi efektif dan tugas yang jelas antar pihak yang terlibat.
3. Proses Atribut 2.2 (*Work Product Management*)
   a. Kebutuhan akan hasil kerja proses ditetapkan.
   b. Kebutuhan untuk dokumentasi dan kontrol dari hasil kerja ditetapkan.
   c. Hasil kerja diidentifikasi dengan baik, didokumentasikan dan dikontrol.
   d. Hasil kerja di ulas kembali sesuai dengan rencana pengaturan dan disesuaikan sesuai kebutuhan untuk mencapai kebutuhan.

Setelah mengetahui nilai pencapaian saat ini, target dan gap, maka diperlukan hal apa saja untuk mendapatkan rekomendasi tata kelola keamanan teknologi informasi yang sesuai.

Simpulan

Berdasarkan hasil penelitian dan penjelasan dari bab sebelumnya, maka penulis dapat menarik kesimpulan, sebagai berikut :

1. Penyertaan keamanan pada tata kelola dilakukan dengan menggunakan COBIT 5 *for information security*, dimana COBIT 5 *for information security* ini merupakan bagian dari family COBIT 5, hanya saja semua enabler proses yang ada pada COBIT 5 dimasukan unsur keamanannya.
2. Dalam menentukkan domain yang akan dipilih dalam pembuatan Tata Kelola Keamanan Teknologi Informasi, maka harus dilakukan penurunan pemilihan domain, dengan perbandingan tujuan kemanan TI Organisasi DISKOMINFO Kota Sukabumi dengan tujuan Organisasi COBIT. Dalam perbandingan ini, diambil dari visi, misi dan tujuan DISKOMINFO, diambil yang berhubungan dengan keamanan teknologi infromasinya. Kemudian dilanjutkan dengan perbandingan E*nterprise goals* (EG) COBIT 5 terpilih dengan IT *Relation Goals (ITRG*) COBIT 5. Setelah itu dilakukan perbandingan antara Tujuan kemanan TI DISKOMINFO dengan *Relation Goals (ITRG*) COBIT 5 terpilih. Dari sini akan terlihat kesesuaiannya. Hasil dari ITRG terpilih, diambil

domain sesuai dengan ITRG mana yang terpilih, hal ini sudah ditentukan oleh COBIT 5. Dari ITRG yang terpilih maka akan terlihat enabler proses yang sesuai dengan ITRG tersebut, dan ini pun sudah ditentukan oleh COBIT.

3. Perancangan model referensi proses dan kapabilitas nilai menggunakan COBIT 5 *for information security dan Process Assessment Model* (PAM) COBIT 5. Dalam COBIT 5 for information Security setiap enablernya akan dikaitkan dengan kemanan informasi. Untuk implementasinya diambil satu EG terpilih, dan disana domain yang dipilih sesuai dengan fokus tujuan dari DISKOMINFO Kota Sukabumi. Diambil perwakilan domain dari ITRG terpilih, yaitu ada 7 domain, diantaranya EDM01, APO01, APO02, APO03, BAI02, DSS03 dan DSS05. Dan ada 133 *best practise.*

4. Dari hasil penilaian kondisi saat ini didapatkan pada domain EDM01, APO03, DSS03 dan DSS05 berada pada level 0, dimana presentase pencapaiannya >15-50 %, disini sudah adanya beberapa bukti pendekatan dan beberapa pencapaian, atribut yang ditetapkan dalam proses penilaian, dan beberapa belum bias diprediksi. Sedangkan domain APO01, APO02 dan BAI02 berada pada level 1, dengan *average score Best Practise* dan *work product* presentase pencapaiannya berada pada > 50-85%, disini sudah adanya bukti pendekatan sistematik dan pencapaian yang signifikan dan adanya penetapan atribut dalam proses penilaian. Dari presentase pencapaian dan target, maka akan munculah kesenjangan, dan pada Tata Kelola Keamanan teknologi informasi dilakukan dengan memperhatikan detail perbedaan antara kondisi saat ini, dengan target level yang ingin dicapai. Dalam implementasinya, maka hal ini dirancang sesuai dengan tahapan level yang ingin dicapai, dan dengan membuat roadmap sesuai dengan pencapaian level setiap domain.

Daftar Pustaka

Asriyanik. 2015. Tesis Tata kelola Teknologi Informasi Perguruan Tinggi. Bandung : Unla.

Eko Indrajit, Richardus, Prof. 2016. *Tata Kelola Teknologi Informasi edisi ke dua*. Yogyakarta. Preinexus.

Hasan, M.Iqbal, M.M. 2012. *Pokok-Pokok Materi Metode Penelitian Dan Aplikasinya*. Bogor : Ghalia Indonesia.

ISACA. 2008. *Overview of International IT Guidance* .IT *Governance Institute.*

ISACA. 2000. *COBIT (3rd Edition) Implementation Tool Set. COBIT Steering Committee and the IT Governance Institute.*

Susendro, Kristianto. 2009. *implementasi tata kelola teknologi informasi* Bandung *: Informatika.*.

Republik Indonesia. 2016. Peraturan Walikota Sukabumi No. 44 Tentang Kedudukan, Susunan Organisasi, Tugas Pokok, Fungsi, dan tata Kerja Dinas Komunikasi dan Informatika. Walikota Sukabumi. Sukabumi.

Republik Indonesia. 2016. Peraturan Mentri Komunikasi dan Informatika No. 4 Tentang Sistem Manajemen Pengamanan Informasi. Kementrian Komunikasi dan Informatika. Jakarta.

Republik Indonesia. 2016. Peraturan Mentri Komunikasi dan Informatika No. 41 Tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi. Kementrian Komunikasi dan Informatika. Jakarta.

willy abdillah, jogiyanto. 2010. *Sistem Tata Kelola Teknologi Informasi.* Andi: Yogyakarta.