PERANCANGAN TATA KELOLA KEAMANAN INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 5 DAN SNI ISO/IEC 27001:2013

INDRA YUSTIANA
DEPARTEMEN SISTEM INFORMASI UNIVERSITAS NUSA PUTRA, SUKABUMI, INDONESIA
e-mail: indra.yustiana@nusaputra.ac.id

ABSTRAK

Pemanfaatan Teknologi Informasi (TI) dalam mendukung terselenggaranya pelayanan yang optimal menjadi kebutuhan utama organisasi saat ini, khususnya pada Badan Perencana Pembangunan Daerah Provinsi Jawa Barat. Akan tetapi, jaminan pengelolaan layanan yang baik dirasa belum maksimal tanpa adanya penggunaan sebuah standar. pemamfaatan teknologi informasi di badan penyelenggara pelayanan publik yang diharapkan tidak hanya kualitas layanannya saja yang meningkat tetapi juga adanya penjaminan keamanan yang sudah di standarkan. Akan tetapi, penggunaan sebuah standard dirasa belum maksimal melihat cakupan yang disediakan kurang luas sehingga diadakannya penggabungan beberapa standar dengan harapan standar-standar tersebut saling melengkapi.

Dalam hal ini pemetaan SNI 27001 kedalam COBIT 5 akan meningkatkan kinerja dari framework dan sejalan dengan regulasi yang berlaku. Klausa SNI 27001 dipetakan kedalam control obyektif COBIT 5 yang berkaitan erat dengan aspek keamanan yaitu EDM03 Jaminan Optimasi Risiko, APO12 Pengaturan Risiko, APO13 Pengaturan Keamanan, BAI06 Pengaturan Perubahan dan DSS05 Manajemen Layanan Keamanan.

Hasil dari penelitian yang didaapat melalui kuisoner dan wawancara menyatakan nilai kapabilitas sistem informasi BAPPEDA Jabar pada pada domain control akses dan media handling ada pada level 2 dan hendak dinaikan ke level 3. Rekomendasi yang diajukan adalah tahapan yang harus dilakukan BAPPEDa untuk menaikan level kapabilitasnya .

Rekomendasi yang diajukan digunakan untuk menyusun dokumen kebijakan keamanan informasi di lingkungan kerja BAPPEDA Jabar pada domain control akses daan media handling

Kata Kunci : SNI 27001, COBIT 5, EDM03, APO12,APO13, BAI06,DSS05, kapabilitas

1. PENDAHULUAN

Informasi adalah sumber daya utama bagi semua organisasi dari waktu diciptakan sampai saat dihancurkan. Pengelolaan kerahasiaan, integritas dan ketersediaan informasi yang efektif sangat penting dalam lingkungan yang serba cepat. Untuk memastikan bahwa siklus hidup informasi dijamin dari sudut pandang keamanan, organisasi harus mampu melacak aliran informasi dalam siklus hidupnya. Untuk membantu hal ini, organisasi dianjurkan

untuk membuat dan mengelola sistem manajemen keamanan informasi (SMKI).

Penerapan SMKI dalam suatu organisasi membutuhkan arahan dan pengawasan agar sejalan dengan visi dan misi dari organisasi, hal ini dapat dilakukan oleh sebuah tata kelola teknologi informasi yang merupakan

kumpulan tanggung jawab dan praktek yang dilakukan oleh dewan dan manajemen eksekutif dengan tujuan memberikan arahan strategis, memastikan bahwa tujuan tercapai, memastikan bahwa risiko dikelola secara tepat dan memverifikasi bahwa sumber daya organisasi itu digunakan secara bertanggung jawab [1]. Kerangka kerja tata kelola TI memberikan bimbingan tentang tata kelola, manajemen dan operasi TI di organisasi sejalan dengan tujuan organisasi tersebut. Kerangka tata kelola akan membantu manajemen menetapkan peran, memperjelas tanggung jawab dan menetapkan akuntabilitas untuk pengambilan keputusan yang berdampak pada pencapaian organisasi tujuan strategis.

Keamanan informasi merupakan bagian dari tanggung jawab tata kelola organisasi/organisasi yang diimplementasikan kedalam bentuk tata kelola keamanan informasi(TKKI), Tata kelola keamanan Informasi (Information Security Governance) adalah bagian dari tata kelola organisasi/organisasi yang memberikan arahan strategi, memastikan bahwa tujuan organisasi dicapai, mengelola resiko, menggunakan sumber daya organisasi secara bertanggung jawab, dan mengawasi berhasil atau gagalnya program keamanan [2], sedangkan menurut Bowen TKKI adalah proses membangun dan memelihara kerangka kerja untuk memberikan jaminan bahwa strategi keamanan informasi selaras dengan dan mendukung tujuan bisnis, konsisten dengan hukum dan peraturan yang berlaku melalui kepatuhan terhadap kebijakan dan pengendalian internal, dan memberikan penugasan tanggung jawab, semua dalam upaya untuk mengelola risiko [3].

Salah satu sektor yang menerapkan IT adalah badan penyelenggara pelayanan public yang tata kelola IT-nya diatur oleh Peraturan Menteri Komunikasi Dan Informatika Nomor: **41/**PER/MEN.KOMINFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional, sedangkan manajemen keamanannya diatur oleh Peraturan Menteri Komunikasi Dan Informatika Nomor: 4/PER/MEN. KOMINFO/2014 Tentang Sistem Manajemen Pengamanan Informasi. Hal ini menggambarkan bagaimana pentingnya tata kelola teknologi informasi beserta praktek-praktek keamanannya. Penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan *(integrity*) dan ketersediaan (*availability*).

Salah satu badan penyelenggara pelayanan publik yaitu BAPPEDA Jabar, salah satu tugas yang dipunyainya adalah mewujudkan keselarasan perencanaan pembangunan Provinsi Jawa Barat dengan fungsi perencanaan daerah (Kabupaten/Kota) dan pusat serta perencanaan pembangunan yang konsisten dan transparan. Untuk mewujudkan dua hal tersebut BAPPEDA menerapkan sistem informasi yang membantu pemerintah daerah c.q. Badan Perencanaan dan Pembangunan Daerah dalam menyusun rencana kerja tahunan yang diselaraskan dengan Rencana Pembangunan Jangka Menengah Daerah. Partisipasif dan transparansi bagi setiap stakeholder maupun publik dalam menyampaikan usulan yang menjadi bahan pertimbangan rencana kerja pemerintah daerah merupakan keunggulan yang ditawarkan. Salah satu yang sistem informasi yang dipunya badan ini adalah RKPD Online yang merupakan wadah kolaborasi dalam melakukan penyusunan rencana kerja berbasis sistem informasi. Seluruh usulan yang akan menjadi rencana kerja akan teradministrasi dengan baik melalui satu pintu, sehingga tidak akan ada usulan yang tidak tercatat di sistem.

Dalam sistem ini integrasi, kerahasiaan dan ketersediaan data usulan menjadi sangat penting karena mencegah terjadinya kesalahan anggaran ,keterlambatan proses penganggaran dan jual beli usulan oleh fihak-fihak yang tidak bertanggung jawab. Kebocoran informasi ini biasanya terjadi akibat lemahnya pengaturan hak akses dan kultur user yang kurang memperhatikan atau awam tentang keamanan informasi dalam hal ini tentang *media handling*, serta insiden keamanan lainnya terkait teknologi informasi yang diterapkan. Masalah yang muncul tersebut digunakan untuk menentukan prioritas prosedur untuk meminimalkan risiko.

Langkah pertama dalam membangun sebuah tata kelola yang efektif adalah pembentukan metodologi implementasi yaitu penerapan kerangka kerja tunggal yang terintegrasi dalam penelitian ini diimplementasikan dengan pemetaan klausul-klausul SNI ISO/IEC 27001:2013 (selanjutnya disebut SNI 27001) pada proses COBIT 5 sehingga memperkuat aspek tata kelola keamanan informasi sehingga dapat memberikan arahan strategi, memastikan bahwa tujuan organisasi dicapai, mengelola resiko, menggunakan sumber daya secara bertanggung jawab, dan mengawasi berhasil atau gagalnya program keamanan COBIT (Control Objective for Information & Related Technology) 5, COBIT merupakan kumpulan IT best practice untuk tata kelola IT yang dapat membantu pengguna, manajemen organisasi dan stakeholder dalam menganalisa kesenjangan (gap) antara kebutuhan bisnis, kebutuhan control dan kebutuhan teknis. COBIT mencakup topik yang jauh lebih besar terkait dengan tata kelola teknologi informasi, dan biasanya digunakan sebagai bagian dari keseluruhan kerangka tata kelola organisasi namun tidak memiliki banyak persyaratan keamanan informasi yang terperinci seperti SNI 27001. Sehingga integrasi keduanya dapat menurunkan keseluruhan biaya untuk menjaga tingkat keamanan yang dapat diterima, mengelola risiko secara efektif dan mengurangi tingkat risiko secara keseluruhan. Selain itu, integrasi ini juga akan mengurangi kebingungan dan penyimpangan yang ada antara IT dan Audit [4].

Onifade menyatakan bahwa integrasi kerangka kerja ini akan membuat perbaikan pada efektivitas operasional, uptime dan ketersediaan, kualitas layanan, control organisasi dan manajemen, manajemen risiko dan jaminan serta pelaporan berkala dan keberlangsungan bisnis [5]].

Penentuan masalah dilakukan dengan metode penyampaian kuesioner kepada pegawai Biro TI BAPPEDA Jabar. Kuesioner tersebut mengadopsi Control Obyektif pada kerangka kerja kerja COBIT 5 yang telah diperkaya dengan klausa-klausa pada standar SNI 27001. Hasil kuesioner tersebut dianalisa untuk mendapatkan masalah yang signifikan sesuai dengan risk map.

Hasil dari penelitian ini adalah sebuah tata kelola pelaksanaan keamanan informasi, yang berupa kumpulan kebijakan keamanan informasi yang berhubungan dengan pengelolaan asset informasi dan telah mempertimbangkan masalah yang signifikan. Unsur-unsur dokumen tata kelola keamanan informasi berisi pernyatan komitmen, tujuan, ruang lingkup, rincian kebijakan, definisi, catatan rilis dan akan dijadikan dasar untuk penyusunan dokumen kebijakan tata kelola informasi di lingkungan kerja BAPPEDA Jabar.

2. METODOLOGI

Untuk memperoleh data yang diperlukan maka penulis mengunakan metode sebagai berikut [6]:

a. Penelitian lapangan (Field Research),yaitu penelitianyang dilakukan untukmengumpulkan data primer melalui observasi dengan cara memberikan kuesioner kepada responden.
b. Penelitian kepustakaan (Library Research), yaitu yang dilakukan dengan membaca buku-buku yang berhub-

ungan dengan masalah yang diteliti ataupun dengan cara browsing di internet untuk mencari artikel-artikel atau data-data yang dapat membantu hasil dari penelitian

Data yang diperoleh pada penelitian ini ada dua jenis yaitu data kuantitatif dan kualitatif, data kuantitatif diperoleh pada saat kuesioner sedangkan data kualitatif diperoleh melalui wawancara Sumber data yang menjadi bahan analisis dalam penelitian ini dapat dibedakan menjadi dua yaitu :

a. Data primer yaitu data yang didapat dari sumber pertama seperti hasil wawancara atau hasil pengisian kuesioner
b. Data sekunder yaitu data primer yang telah diolah lebih lanjut dan disajikan baik oleh pengumpul data primer maupun pihak lain.

Sampel data yang akan diambil dalam penelitian ini dihitung berdasarkan diagram Nomogram Harry[7] . Jumlah populasi karyawan Bappeda sekitar 300 orang , sampel diambil dengan tingkat kepercayaan 95% maka di dapat jumlah sampel = 35% x 300 x 1.195 = 125.475 dibulatkan jadi 125 sampel.

.

Uji Validitas dan Reliabilitas

Dalam sebuah penelitian kuantitatif dengan pengumpulan data secara angket melakukan uji validitas merupakan sebuah keharusan, dimana uji ini untuk mengetahui apakah angket yang dilaksanakan benar-benar valid untuk mengukur variable yang diteliti. Dalam penelitian ini digunakan uji validitas dengan 2 metode yaitu korelasi Bevariate Pearson's. Analisis ini dengan cara mengkorelasikan masing-masing skor item dengan skor total. Skor total adalah penjumlahan dari keseluruhan item. Item-item pertanyaan yang berkorelasi signifikan dengan skor total menunjukkan item-item tersebut mampu memberikan dukungan dalam mengungkap apa yang ingin diungkap valid. Jika r hitung ≥ r tabel (uji 2 sisi dengan sig. 0,05) maka instrumen atau item-item pertanyaan berkorelasi signifikan terhadap skor total (dinyatakan valid) [7]. Uji validitas menggunakan alat bantu SPSS for Windows versi 19.00.

Reliabilitas (reliability) adalah tingkat seberapa besar suatu pengukur mengukur dengan stabil dan konsisten. Besarnya tingkat reliabilitas ditunjukkan oleh koefisiennya, yaitu koefisien reliabilitas. Teknik yang digunakan untuk mengukur reliabilitas pengamatan adalah Cronbach Alpha dengan cara membandingkan nilai alpha dengan standarnya, dengan ketentuan jika [7] :

1. Nilai Cronbach Alpha 0,00 s.d. 0,20, berarti kurang reliabel
2. Nilai Cronbach Alpha 0,21 s.d. 0,40, berarti agak reliabel
3. Nilai Cronbach Alpha 0,42 s.d. 0,60, berarti cukup reliabel
4. Nilai Cronbach Alpha 0,61 s.d. 0,80, berarti reliabel
5. Nilai Cronbach Alpha 0,81 s.d. 1,00, berarti sangat reliabel

Tahap Penelitian

Merupakan rangkaian tahapan sistematis yang dilakukan untuk menyelesaikan dan menjawab pertanyaan penelitian ini yang telah ditentukan. Rangkaian tahapan pada metodologi penelitian ini terdiri dari 8 tahapan, meliputi :

1. Tahap persiapan

   Merupakan rangkaian sebelum memulai pengumpulan dan pengolahan data. Dalam tahap ini di susun hal-hal yang harus dilakukan dengan tujuan efektivitas waktu dan pekerjaan tugas akhir. Dalam tahap ini dilakukan studi literature yang merupakan penelusuran literatur yang bersumber dari buku, media, pakar ataupun dari hasil penelitian orang lain yang bertujuan untuk menyusun dasar teori yang kita gunakan dalam melakukan penelitian. Pada tahap ini juga akan ditentukan ruang lingkup control obyektif yang terkait dengan

dengan keamanan informasi pada control obyektif yang ada di kerangka kerja COBIT 5.

2. Tahap pemetaan ISO 27001 : 2013 ke Kontrol Obyektif terpilih
   Pada tahap ini dilakukan pemetaan klausul-klausul pada ISO 27001:2013 ke dalam control obyektif yang terpilih yaitu APO13 sebagai control obyektif yang berkaitan dengan pengaturan keamanan dan EDM03, APO12, BAI06 dan DSS05 yang merupakan control obyektif yang terkait dengan APO13.
3. Tahap Pemilihan proses
   Pada langkah ini akan dipilih proses-proses control obyektif pada COBIT dengan melakukan memetakan visi dan dan misi organisasi dengan tujuan penerapan IT sehingga didapat control obyektif yang berkesesuaian dengan tujuan organisasi.
4. Tahap Pengukuran kinerja saat ini
   Hal ini dilakukan untuk mengetahui kondisi existing dari kinerja, sehingga dapat digunakan sebagai patokan dalam melakukan rekomendasi perbaikan. Pada tahap ini dilaksanakan kuesioner untuk tiap control obyektif yang terpilih
5. Penetapan kinerja yang diharapkan
   Menetapkan kinerja harapan yaitu kinerja yang diharapkan dalam pengelolaan teknologi informasi
6. Analisa gap atau kesenjangan
   Langkah ini diperlukan untuk menganalisa kesenjangan dari hasil pengukuran kinerja saat ini dengan kinerja harapan.
7. Rencana Perbaikan Proses Tata Kelola TI
   Langkah ini diperlukan sesuai dengan komponen tata kelola TI berdasarkan kerangka kerja COBIT.
8. Penyusunan Dokumen Tata Kelola TI
   Langkah ini menghasilkan output dari penelitian yang dilakukan adalah penyusunan dokumen tata kelola TI sesuai dengan langkah-langkah yang telah di lakukan.

3. HASIL DAN PEMBAHASAN

Pemetaan SNI ISO/IEC 27001 ke Dalam Kontrol Obyektif COBIT 5, Penggabungkan kerangka kerja COBIT 5 dan standar keamanan informasi SNI ISO 27001 dengan cara memetakan klausul pada SNI ISO 27001 ke dalam control obyektif COBIT 5. Control obyektif yang dipilih adalah EDM03 Optimasi Risiko, APO12 Manajemen Risiko, APO13 Manajemen Keamanan, BAI06 Manajemen Perubahan dan DSS05 Pengaturan Pelayanan Keamanan, pemilihan control obyektif ini berdasarkan pemetaan tujuan terkait IT COBIT 5 dengan proses yang bernilai proses utama [8].

Tabel 1 pemetaan SNI ISO/IEC 27001 kedalam control obyektif EDM03

EDM03 Jaminan Optimasi Risiko					
SUB	DESKRIPSI	SNI ISO/IEC 27001 : 2013		Annex	
EDM03.1	Evaluasi manajemen risiko	9.3	Manajemen Review	A.5.1.2	review kebijakan keamanan informasi
EDM03.2	Arahan manajemen risiko	4.3	Menentukan ruang lingkup ISMS		
		5.1	Kepemimpinan dan komitmen		
		5.2	Kebijakan	A.5.1.1	kebijakan keamanan informasi
				A.6.2.1	kebijakan perangkat mobile
				A.9.1.1	kebijakan akses kontrol
				A.10.1.1	kebijakan penggunaan kontrol kriptografi
				A.14.2.1	kebijakan pengembangan sistem informasi yang aman
				A.15.1.1	kebijakan keamanan informasi untuk hubungan dengan suplier
		7.4	komunikasi	A.13.2	transfer informasi
EDM03.3	Monitoring Manajemen risiko	9.1	Pengawasan, pengukuran,analisis dan evaluasi	A.18.2	review keamanan informasi
		9.2	audit internal	A.12.7	pertimbangan audit sistem

Tabel 2 Pemetaan SNI ISO/IEC 27001 kedalam control obyektif APO012

APO12 Manajemen Risiko					
SUB	DESKRIPSI	SNI ISO/IEC 27001 : 2013		ANNEX	
APO12.1	pengumpulan data	6.1.2	Penilaian risiko keamanan informasi	A.8.1	tanggung jawab asset
APO12.2	analisis risiko			A.8.2	klasifikasi informasi
APO12.3	maintain profil risiko			A.14.1.1	spesifikasi dam analisis kebutuhan keamanan informasi
APO12.4	artikulasi risiko				
APO12.5	penentuan portofolio aksi manajemen risiko	4.2	memahami kebutuhan dan harapan fihak terkait	A.18.1.1	identifikasi peraturan yang diterapkan dan persyaratan kontrak
		5.3	peran , tanggung jawab dan otoritas organisasi	A.18.2.2	pemenuhan dengan kebijakan dan standar keamanan
APO12.6	respon terhadap risiko	6.1.3	Penanganan risiko keamanan informasi	A.16	manajemen insiden keamanan informasi dan perbaikannya
		7.1	pengadaan sumber daya	A.7	keamanan sumber daya manusia

Tabel 1 pemetaan SNI ISO/IEC 27001 kedalam control obyektif APO013

APO13 Manajemen Keamanan					
SUB	DESKRIPISI	SNI ISO/IEC 27001 : 2013		Annex	
APO13.1	pembangunan dan perawatan ISMS	4.1	Memahami organisasi dan konteknya	A.6.1	Organisasi internal
		4.2	Memahami kebutuhan dan harapan pihak terkait		
		4.4	ISMS		
		7.2	kompetensi	A.7.2.2	pelatihan, pendidikan dan peningkatan kesadaran kemanan informasi
		7.3	kesadaran		
		10.2	perbaikan berkesinambungan		
APO13.2	Penentuan dan pengaturan rencana penanganan risiko keamanan informasi	5.3	Peran dan tanggungjawab organisasi	A.14.1	analisis dan spesifikasi kebutuhan keamanan informasi
		6.2	Tujuan keamanan informasi dan perencanaan untuk mencapainya	A.17	manajemen keamanan informasi dalam aspekkeberlangsungan bisnis
APO13.3	pengawasan dan review ISMS	9.3	manajemen review	A.18.2	review keamanan informasi
		9.2	internal audit		

Tabel 4.pemetaan SNI ISO/IEC 27001 kedalam control obyektif BAI06

BAI06 Manajemen Perubahan					
SUB	DESKRIPISI	SNI ISO/IEC 27001 : 2013		Annex	
BAI06.1	evaluasi , prioritasi,dan otorisasi permintaan perubahan	10	perbaikan	A.12.1.2	Manajemen perubahan
BAI06.2	pengaturan perubahan emergensi			A.14.2.2	prosedur kontrol perubahan sistem
BAI06.3	penelusuran dan pelaporan status perubahan			A.14.2.3	review teknis dari aplikasi ketika platform operasi dirubah
BAI06.4	penutupan dan dokumentasi perubahan			A.14.2.4	pembatasan pada perubahan software

Tabel 2 pemetaan SNI ISO/IEC 27001 kedalam control obyektif DSS05

DSS05 Manajemen Layanan Keamanan					
SUB	DESKRIPISI	SNI ISO/IEC 27001 : 2013		Annex	
DSS05.1	Perlindungan terhadap malware	4.4	ISMS	A.12.2	Perlindungan terhadap malware
DSS05.2	Pengaturan keamanan jaringan dan konektivitas			A.13	Keamanan komunikasi
DSS05.3	pengaturan keamanan endpoint			A.6	Perangkat mobile dan teleworking
				A.7	Keamanan Sumber daya manusia
DSS05.4	pengaturan identitas user dan akses lojik			A.9	kontrol akses
				A.8.2	Klasifikasi informasi
				A.8.1	Tanggung jawab asset
DSS05.5	pengaturan akses fisikal terhadap asset IT			A.11.1	daerah aman
				A.8.1	Tanggung jawab asset
DSS05.6	pengaturan dokumen sensitif dan output devices			A.11.2.7	pembuangan atau penggunaan kembali peralatan secara aman
				A.8.3	penanganan media
DSS05.7	pengawasan terhadap infrastruktur yang berhubungan dengan kejadian keamanan			A.11.2	peralatan
				A.12.4	Logging dan pengawasan
				A.8.1	Tanggung jawab asset

Hasil Penentuan Analisa Kesenjangan

Dengan adanya tingkat kematangan yang sebenarnya (as is) dan target tingkat kematangan yang diinginkan (to be) pada proses-proses terkait , maka akan membentuk suatu kondisi dimana Sistem informasi BAPPEDA Jabar melakukan penyesuaian. Dari perhitungan capability level menunjukkan bahwa nilai Sistem belum mencapai yang diinginkan yang mana tingkat kapabilitas sistem sebenarnya ada di level 2 (dengan beberapa hal yang harus dipenuhi terlebih dahulu).

Tabel 6 Hasil Analisa Kesenjangan

CONTROL OBYEKTIF	CURRENT MATURITY	EXPECTED MATURITY	GAP MATURITY
EDM03 Jaminan Optimasi Risiko	1,84	3	1,16
APO12 Manajemen Risiko	1,8	3	1,2
APO13 Manajemen Keamanan	1,97	3	1,03
BAI06 Manajemen Perubahan	1,83	3	1,17
DSS05 Manajemen Layanan Keamanan	1,88	3	1,12

Perumusan Kebijakan Keamanan Informasi. Adapun kebijakan keamanan informasi yang diperoleh yaitu berupa :

1. Prosedur control akses
   Semua Sistem Bisnis BAPPEDA harus mengembangkan, mengadopsi atau mematuhi prosedur pengendalian akses formal dan terdokumentasi yang membahas tujuan, ruang lingkup, peran, tanggung jawab, komitmen manajemen, koordinasi antara entitas organisasi, dan kepatuhan.

2. Manajemen Akun
   a. Mengidentifikasi jenis akun (yaitu, individu, grup, sistem, aplikasi, tamu / anonim, dan sementara).
   b. Menetapkan kondisi untuk keanggotaan kelompok
   c. Mengidentifikasi pengguna yang berwenang atas aset informasi dan menentukan hak akses.
   d. Meminta persetujuan yang sesuai untuk permintaan untuk membuat akun.
   e. Menetapkan, mengaktifkan, memodifikasi, menonaktifkan, dan menghapus akun.
   f. Secara khusus mengotorisasi dan memantau penggunaan akun tamu / anonim dan sementara.
   g. Beri tahu manajer akun saat akun sementara tidak lagi diperlukan dan saat pengguna aset informasi dihentikan, dipindahkan, atau penggunaan aset informasi.
   h. Menonaktifkan akun sementara yang tidak lagi diperlukan dan akun

pengguna yang dihentikan atau ditransfer.

i. Berikan akses ke sistem berdasarkan (1) otorisasi akses yang valid, (2) penggunaan sistem yang diinginkan, dan (3) atribut lain yang dipersyaratkan oleh organisasi atau misi / fungsi bisnis yang terkait.
j. Tinjau ulang akun secara periodik atau setidaknya setiap tahun

3. Penegakan Akses
Semua Sistem Bisnis BAPPEDA harus menerapkan otorisasi yang disetujui untuk akses logis ke sistem sesuai dengan kebijakan yang berlaku

4. Penegakan Arus Informasi
Semua Sistem Bisnis BAPPEDA harus menerapkan otorisasi yang disetujui untuk mengendalikan arus informasi di dalam sistem dan antara sistem yang saling terkait sesuai dengan kebijakan yang berlaku.

5. Pemisahan Tugas
a. Pisahkan tugas individu jika diperlukan, untuk mencegah aktivitas jahat tanpa kolusi.
b. Dokumen pemisahan tugas.
c. Mengimplementasikan pemisahan tugas melalui otorisasi akses aset informasi yang diberikan

6. Concurrent Session Control
Semua Sistem Bisnis BAPPEDA harus membatasi jumlah sesi bersamaan untuk setiap akun sistem menjadi sepuluh untuk aset informasi

7. Kunci Sesi
Semua Sistem Bisnis BAPPEDA harus mencegah akses lebih jauh ke aset informasi dengan memulai kunci sesi setelah 120 menit tidak aktif atau setelah menerima permintaan dari pengguna. Selain itu, Sistem Bisnis BAPPEDA harus mempertahankan kunci sesi sampai pengguna membangun kembali akses dengan menggunakan prosedur identifikasi dan otentikasi yang telah ditetapkan

8. Tindakan yang Diijinkan tanpa Identifikasi atau Otentikasi: Semua Sistem Bisnis BAPPEDA harus mengidentifikasi tindakan pengguna tertentu yang dapat dilakukan pada aset informasi tanpa identifikasi atau otentikasi. Selain itu, Sistem Bisnis BAPPEDA harus mendokumentasikan dan memberikan alasan pendukung dalam rencana keamanan untuk aset informasi, tindakan pengguna yang tidak memerlukan identifikasi dan otentikasi

9. Akses Jarak Jauh: Semua Sistem Bisnis BAPPEDA harus:
a. Dokumentasi memungkinkan metode akses jarak jauh ke aset informasi.
b. Tetapkan batasan penggunaan dan panduan pelaksanaan untuk setiap metode akses jarak jauh yang diizinkan.
c. Pantau akses jarak jauh yang tidak sah ke aset informasi.
d. Otorisasi akses jarak jauh ke aset informasi sebelum koneksi.
e. Terapkan persyaratan untuk koneksi jarak jauh ke aset informasi.

10. Akses Nirkabel
a. Tetapkan batasan pemakaian dan panduan pelaksanaan akses nirkabel.
b. Pantau akses nirkabel yang tidak sah ke aset informasi.
c. Otorisasi akses nirkabel ke aset informasi sebelum koneksi.
d. Terapkan persyaratan untuk koneksi nirkabel untuk aset informasi

11. Kontrol Akses untuk Perangkat Mobile
a. Menetapkan batasan penggunaan dan panduan implementasi untuk perangkat mobile yang dikendalikan oleh organisasi.
b. Otorisasi koneksi perangkat mobile yang memenuhi batasan penggunaan organisasi dan pan-

duan pelaksanaan untuk aset informasi organisasi.

c. Pantau koneksi perangkat mobile yang tidak sah ke aset informasi organisasi.
d. Terapkan persyaratan untuk koneksi perangkat mobile ke aset informasi organisasi.
e. Nonaktifkan fungsi aset informasi yang menyediakan kemampuan untuk eksekusi kode secara otomatis pada perangkat mobile tanpa arahan pengguna
f. Terbitkan perangkat seluler yang dikonfigurasi secara khusus ke individu yang bepergian ke lokasi (lokasi internasional yang dianggap sensitif oleh Departemen Luar Negeri) bahwa organisasi dianggap memiliki risiko signifikan sesuai dengan kebijakan dan prosedur organisasi

12. Penggunaan Sistem Informasi Eksternal. Semua Sistem Bisnis BAPPEDA harus menetapkan syarat dan ketentuan, sesuai dengan hubungan kepercayaan yang dibuat dengan organisasi lain yang memiliki, mengoperasikan, dan / atau memelihara aset informasi eksternal, yang mengizinkan orang yang berwenang untuk:
    a. Akses aset informasi dari sistem informasi eksternal.
    b. Memproses, menyimpan, dan / atau mengirimkan informasi yang dikendalikan organisasi dengan menggunakan sistem informasi eksternal

13. Konten yang Dapat Diakses Publik
    a. Tetapkan individu yang berwenang untuk mengirimkan informasi ke sistem informasi organisasi yang dapat diakses oleh publik.
    b. Latih orang yang berwenang untuk memastikan bahwa informasi yang dapat diakses publik tidak mengandung informasi non publik.
    c. Tinjau kembali isi informasi publik yang dapat diakses untuk informasi non publik sebelum dikirim ke sistem informasi organisasi
    d. Tetapkan individu yang berwenang untuk mengirimkan informasi ke sistem informasi organisasi yang dapat diakses oleh publik.
    e. Latih orang yang berwenang untuk memastikan bahwa informasi yang dapat diakses publik tidak mengandung informasi non publik.
    f. Tinjau kembali isi informasi publik yang dapat diakses untuk informasi non publik sebelum dikirim ke sistem informasi organisasi
14. Media (baik elektronik ataupun non elektronik)yang berisi informasi sensistif harus :
    a. Dalam penyimpanannya harus mengikuti prosedur yang berlaku
    b. Pembuangan atau pengambilan dan pemindahan harus mendapat ijin dari otoritas yang ditunjuk

4. KESIMPULAN

Berdasarkan hasil pengerjaan tesis ini, terdapat beberapa kesimpulan sebagai berikut :

1. Standar best practice SNI 27001:20013 hanya berfokus pada proses implementasi SMKI sedangkan COBIT 5 berorientasi pada proses bisnis dan tata kelola TI. Untuk membuat dokumen tata kelola keamanan informasi diperlukan proses pengelolaan yang berorientasi proses bisnis serta berfokus pada implementasi SMKI. Untuk itu, diperlukan pemetaan antara SNI 27001:20013 dan COBIT 5. Hasil dari pemetaan SNI 27001:2005 terhadap COBIT 5 menunjukkan bahwa pemetaan ini mampu melingkupi seluruh aktivitas proses keamanan dan praktek kunci keamanan informasi, tidak hanya pada aktivitas implementasi SMKI, namun juga mampu melingkupi proses keamanan yang berorientasi proses bisnis dan tata kelola TI meliputi perencanaan, penyelarasan dengan proses bisnis dan tujuan bisnis, serta

pengorganisasian keamanan informasi.

2. Dari hasil perhitungan kapabilitas BAPPEDA didapat nilai di level 2 namun secara nyatanya masih ada kekurangan untuk mencapai level 2 yaitu lemahnya dokumentasi dan legalitas dalam produk praktek keamanan.
3. Penelitian ini menghasilkan ini rekomendasi terkait keamanan informasi pada domain control akses dan *media handling* yang digunakan untuk menyusun dokumen tata kelola keamanan informasi dan struktur oraganisasi BAPPEDA yang sudah mewadahi sektor teknologi informasi
4. Rekomendasi yang dihasilkan penelitian ini untuk mencapa level 3 kapabilitas dimana proses-proses keamanan sudah terdefinisi.
5. Dokumen tata kelola yang dihasilkan berupa kebijakan keamanan informasi pada domain control akses dan media handling

.

REFERENSI

[1] Pironti, John. (2006). Information Security Governance Motivation, Benefit and Outcome, Information Control Journal, ISACA

[2] Love, Paul. et all. (2010). Information Security Governance, Global Technology Audit Guide 15

[3] Bowen, P. et all, (2006). Information Security Handbook: A Guide for Managers (NIST Special Publication 800-100

[4] Modhiri, N and Sheikhpour. R (2012). An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls , International Journal of Security and Its Applications Vol. 6, No. 2

[5] Onifade, O. (2015). Implementing an ISO-integrated Management System Using COBIT 5, COBIT Focus

[6] Kothari, C. R , (2004) Research Methodology : Methods and Techniques, 2nd Revition Edition , College of Commerce University of Rajashtan, New Age International Publisher ISBN (13) : 978-81-224-2488-1

[7] Sugiyono , Statistika untuk Penelitian , (2007) Penerbit Alfabeta , Bandung17

[8] COBIT 5. (2012). COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT, Personal Copy of: Mr. Junjie Qi