EVALUASI TATA KELOLA TEKNOLOGI INFORMASI DAN PERANCANGAN KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 DAN SNI ISO/IEC 27001 (Studi Kasus POLRESTABES BANDUNG)

, Yus Jayusman[1,] Tarmin Abdulghani[2]
[3] *Teknik Informatika, STMIK Bandung*
Jl. Cikutra 113 Bandung Jawa Barat, Indonesia
[2] *Teknik Informatika, Universitas Suryakancana*
Jl. Raya Pasirgede, Cianjur, Jawa Barat, Indonesia
[1]*yusjayusman@gmail.com,* [2]*tarmin@artagani.com*

ABSTRAK

***Intisari*— Dengan semakin pesatnya perkembangan ilmu pengetahuan dan teknologi dewasa ini, sangat berpengaruh terhadap kemajuan bisnis, baik secara individual, swasta, instansi pemerintah termasuk kepolisian. Perkembangan informasi mempunyai peranan yang sangat penting didalam suatu usaha menciptakan kemajuan di semua bidang yang diperuntukan bagi kepentingan manusia pada umumnya. TIK merupakan salah satu bagian penting dalam meningkatkan produktifitas atau layanan, baik dalam memperoleh informasi, mengolah, dan mengunakan informasi tersebut. Polrestabes Bandung mengunakan teknologi informasi untuk melakukan berbagai aktifitas. Contoh yang umum adalah pemanfaatan teknologi informasi untuk pencatatan tindakan kriminal, Izin penggunaan bahan peledak, sistem informasi untuk pembuatan SIM, dan lain-lain.**

Tata kelola teknologi informasi dan Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) sebagai standar keamanan Informasi dalam organisasi, sehingga semua faktor dan dimensi yang berhubungan dengan penggunaan teknologi informasi menjadi bersinergi dan bisa memberikan nilai tambah yang diharapkan bagi perusahaan atau instansi. Berkaitan dengan hal tersebut penulis bermaksud untuk melakukan evaluasi terhadap pelaksanaan tata kelola TI serta mengambil hasil untuk dapat dijadikan pedoman dalam merencanakan suatu kebijakan keamanan informasi berdasarkan keranga kerja COBIT 5 dan ISO/IEC 27001. Perencanaan kebijakan keamanan informasi dibuat untuk dapat meningkatkan kinerja dan layanan TI pada Porestabes Bandung agar terhindar dari segala bentuk ancaman, kerentanan serta memiliki prosedur yang baik dalam menjalankan tata kelola teknologi informasi.

Dalam proses evaluasi tata kelola teknologi informasi dan perencanaan keamanan informasi tentunya tidak terlepas dari data yang relevan dan informasi yang dimiliki untuk mengetahui tujuan instansi, sehingga dapat dijadikan suatu acuan yang baik dan dapat mengatahui tingkat kematangan proses yang ada. Cara pengumpulan data dilakukan dengan menyebarkan angket untuk mengetahui tingkat kematangan saat ini, agar dapat dilakukan perbaikan dan perencanaan kebijakan yang sesuai dengan tujuan, visi misi organisasi dalam mendukung kinerja yang dijalankan oleh Polrestabes Bandung.

Kata kunci : ***Evaluasi Tata kelola TI, COBIT 5, ISO 27001, Polrestabes***

I. PENDAHULUAN

Kehadiran globalisasi membawa pengaruh bagi kehidupan suatu bangsa. Pengaruh globalisasi dirasakan di berbagai bidang kehidupan seperti kehidupan politik, ideologi, ekonomi, sosial budaya, pertahanan keamanan dan lain-lain yang akan mempengaruhi nilai-nilai nasionalisme bangsa. Secara umum globalisasi dapat dikatakan suatu proses tatanan masyarakat yang mendunia dan tidak mengenal batas wilayah. Sebagai sebuah proses, globalisasi berlangsung melalui dua dimensi, dalam interaksi antar bangsa, yaitu dimensi ruang dan dimensi waktu.

Dimensi ruang yang dapat diartikan jarak semakin dekat atau dipersempit sedangkan waktu makin dipersingkat dalam interaksi dan komunikasi pada skala dunia. Hal ini tentunya tidak terlepas dari dukungan pesatnya laju perkembangan teknologi yang semakin canggih khususnya teknologi informasi dan komunikasi (TIK)

Dengan semakin pesatnya perkembangan ilmu pengetahuan dan teknologi dewasa ini, sangat berpengaruh terhadap kemajuan bisnis, baik secara individual, swasta, instansi pemerintah termasuk kepolisian. Perkembangan informasi mempunyai peranan yang sangat penting didalam suatu usaha menciptakan kemajuan di semua bidang yang diperuntukan bagi kepentingan manusia pada umumnya. TIK merupakan salah satu bagian penting dalam meningkatkan produktifitas atau layanan, baik dalam memperoleh informasi, mengolah, dan mengunakan informasi tersebut. Seperti halnya studi kasus penelitian yang dilakukan saat ini, yaitu di Polrestabes Bandung.

Polrestabes Bandung mengunakan teknologi informasi untuk melakukan berbagai aktifitas. Contoh yang umum adalah pemanfaatan teknologi informasi untuk pencatatan tindakan kriminal, Izin penggunaan bahan peledak, sistem informasi untuk pembuatan SIM, dan lain-lain. Contoh penerapan teknologi informasi tersebut meliputi penggunakan komputer, kamera digital, perekam sidik jari, identifikasi bahan Peledak,pencetak kartu SIM, pengenalan wajah, dan tentunya penggunaan jaringan Internet dan Intranet. Dengan penerapan teknologi ini maka diharapkan layanan tersebut dapat diselesaikan lebih efektif dan efesien. Ketika Teknologi informasi ini menjadi bagian terpenting dalam tubuh organisasi, maka informasi ini menjadi sebuah aset yang harus dilindungi dan dikelola dengan sebaik-baiknya.

Salah satu isu utama dalam pemanfaatan TIK yaitu kurangnya manajemen yang tepat dalam asset informasi. Hilangnya Aset Informasi merupakan bencana yang dapat mengakibatkan kerugian finansial bagi perusahaan / Instansi Pemerintah. Untuk menjaga agar aset informasi menjadi penambah nilai dalam sebuah perusahaan atau institusi, maka perlu adanya tata kelola teknologi informasi dan Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) sebagai standar keamanan Informasi dalam organisasi, sehingga semua faktor dan dimensi yang berhubungan dengan penggunaan teknologi informasi menjadi bersinergi dan bisa memberikan nilai tambah yang diharapkan bagi perusahaan atau instansi.

Untuk perancangan SMKI pada Polrestabes Bandung maka terlebih dahulu perlu dilakukan evaluasi terhadap tata kelola teknologi informasi saat ini, dengan tujuan untuk mengetahui tingkat kapabilitas (capability Level) tata kelola teknologi informasi dan proteksi terhadap asset informasi. Untuk mengetahui kapabilitas tata kelola teknologi informasi, maka pada tahapan pertama akan dilakukan evaluasi tata kelola teknologi informasi menggunakan framework COBIT 5 sebagai Tata kelola TI Perusahaan / Governance of Enterprise I T (GEIT).

Tingkat kapabilitas tata kelola ini selanjutnya akan d ijadikan dasar dalam perancangan kebijakan SMKI. Kerangaka kerja yang digunakan yaitu SNI ISO/IEC 27001 : 2009 dengan pertimbangan sebagai berikut :

1. Merupakan sistem manajemen keamanan informasi (SMKI) yang mencakup semua jenis organisasi (komersil , Pemerintah, Nir-laba)
2. Mengadopsi pendekatan P-D-C-A
3. Berbasis Analisis Risiko.
4. Kompatible dengan Sistem Manajemen Keluaran ISO, ISE/IEC, ISO/TS, OHSAS, BS/PAS, TL.
5. Versi ini masih relevan untuk mengakomodir kebutuhan kebutuhan dalam perancangan kebijakan SMKI pada studi kasus di Polrestabes Bandung.

II. KAJIAN PUSTAKA

A. Evaluasi

Pengertian evaluasi menurut para ahli seperti Wrigstone, dkk (1956) mengatakan bahwa evaluasi adalah penaksiran terhadap pertumbuhan dan kemajuan ke arah tujuan atau nilai-nilai yang telah ditetapkan. Sedangkan dalam perusahaan, pengertian evaluasi adalah proses pengukuran akan efektifitas strategi dalam upaya mencapai tujuan bagi perusahaan. Contohnya evaluasi proyek. Hal-hal yang dievaluasi dalam proyek adalah tujuan dan pembangunan proyek, apakah sudah tercapai atau tidak, apakah sesuai dengan rencana atau tidak, jika tidak, apa yang membuatnya tidak tercapai, apa yang harus dilakukan agar sesuai. Hasil yang ditimbulkan dari evaluasi adalah bersifat kualitatif.

Proses evaluasi memiliki tahapan-tahapan, walaupun tahapan setiap objek evaluasi berbeda-beda namun tidak menghilangkan fungsi dari evaluasi itu sendiri. Tahapan-Tahapan Evaluasi secara umum adalah :

1. Menentukan topik evaluasi dalam mengevaluasi tentukan topik atau apa yang akan kita evaluasi baik itu suatu program kerja, atau hasil kerja.
2. Merancang kegiatan evaluasi : sebelum melakukan evaluasi, sebaiknya merancang (desain) kegiatan-kegiatan evaluasi agar tidak ada yang kita lewatkan dalam evaluasi nantinya.
3. Pengumpulan data : Setelah merancang (desain) kegiatan, lakukanlah pengumpulan data sesuai dengan apa yang telah direncanakan dalam kegiatan evaluasi berdasarkan kaidah-kaidah ilmia
4. Pengolahan dan analisis data : Setelah data telah terkumpul, selanjutnya data tersebut diolah dengan mengelompokkan agar mudah dianalisis, dan sediakan tolak ukur waktunya sebagai hasil dari evaluasi.
5. Pelaporan hasil evaluasi : Hasil evaluasi harus diketahui oleh setiap orang-orang yang berkepentingan agar mengetahui hasil-hasil yang telah dia kerjakan

B. Kebijakan

Kebijakan adalah suatu ucapan atau tulisan yang memberikan petunjuk umum tentang penetapan ruang lingkup yang memberi batas dan arah umum kepada seseorang untuk bergerak. Secara etimologis, kebijakan adalah terjemahan dari kata policy. Kebijakan dapat juga berarti sebagai rangkaian konsep dan asas yang menjadi garis pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak. Kebijakan dapat berbentuk keputusan yang

dipikirkan secara matang dan hati-hati oleh pengambil keputusan puncak dan bukan kegiatan-kegiatan berulang yang rutin dan terprogram atau terkait dengan aturan-aturan keputusan

Menurut Budiardjo (1988): kebijakan adalah sekumpulan keputusan yang diambil oleh seorang pelaku atau kelompok politik dalam usaha memilih tujuan-tujuan dan cara-cara untuk mencapai tujuan tersebut.

Menurut Anderson (1979): kebijakan adalah serangkaian tindakan yang mempunyai tujuan tertentu yang mesti diikuti dan dilakukan oleh para pelakunya untuk memecahkan suatu masalah (a purposive corse of problem or matter of concern).

C. Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) atau dalam bahasa Inggris information security management system (ISMS) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau,
mengkaji, memelihara, dan meningkatkan keamanan informasi. SMKI adalah sebuah pendekatan organisasi untuk keamanan informasi. Sebagai sebuah sistem, SMKI harus didukung oleh keberadaan dari hal-hal berikut :

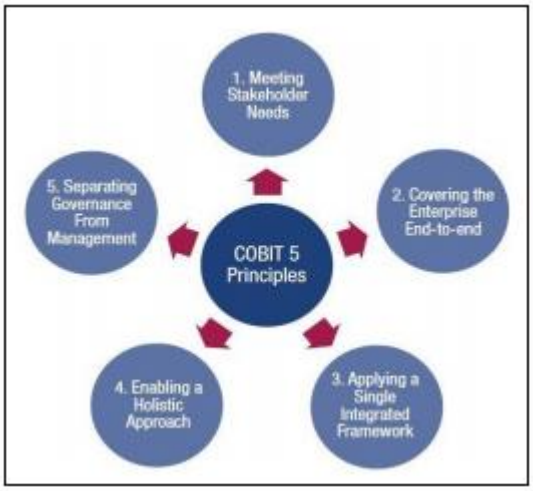
1. Struktur organisas
2. Kebijakan keamanan
3. Prosedur dan proses
4. Tanggung jawab
5. Sumber daya manusia

D. Cobit 5

Control Objective for Information & Related Technology (COBIT) adalah sekumpulan dokumentasi best practice untuk IT Governance yang dapat membantu auditor, pengguna (user), dan manajemen, untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis IT (Sasongko, 2009).

COBIT 5 merupakan generasi terbaru dari panduan ISACA yang membahas mengenai tata kelola dan manajemen IT. COBIT 5 dibuat berdasarkan pengalaman penggunaan COBIT selama lebih dari 15 tahun oleh banyak perusahaan dan pengguna dari bidang bisnis, komunitas IT, risiko, asuransi, dan keamanan. (ISACA 2012:15).

COBIT 5 bersifat umum dan berguna untuk segala jenis ukuran perusahaan, baik itu sektor komersial, sektor non profit atau pada sektor pemerintahan atau publik. COBIT 5 didasarkan pada lima prinsip kunci untuk tata kelola dan manajemen TI perusahaan. Kelima prinsip ini memungkinkan perusahaan untuk membangun sebuah kerangka tata kelola dan manajemen yang efektif, yang dapat mengoptimalkan investasi dan penggunaan TI untuk mendapatkan keuntungan bagi para stakeholder.



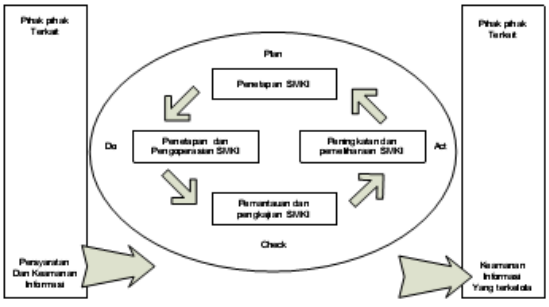
Gambar 2.1.
Lima prinsip dalam COBIT 5

E. SNI ISO / IEC 27001:2009

SNI ISO/IEC 27001:2009 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001: 2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan

Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (review), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya.

Standar ini mengadopsi model “Plan-Do-Chect-Act” (PDAC), yang diterapkan untuk membentuk keseluruhan proses SMKI. Gambar dibawah ini memperlihatkan persyaratan kamanan informasi dan harapan dari pohak terkait menjadi masukan bagi SMKI, serta melalui tindakan dan proses yang diperlukan menghasilkan keluaran keamanan informasi uang memenuhi persyaratan dan harapan tersebut. Gamber tersebut juga memperlihatkan korelasi antara proses-proses yang dituangkan dalam kalusul 4,5,6,7 dan 8 pada SNI ISO/IEC 27001: 2009



Gambar 2.2
Model PDAC dalam aplikasi Proses SMKI

III. METODE PENELITIAN

A. Metode Pemilihan *Sample*

Menurut Sugiyono (2006:57) "Populasi adalah generalisasi dari objek/subjek yang mempunyai karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulan". Dapat disimpulkan bahwa populasi adalah sesuatu yang akan menjadi objek penelitian. Berdasarkan pengertian diatas, maka yang menjadi populasi dalam penelitian ini adalah pegawai/anggota di Polrestabes Bandung.

Menurut Suharsimi Arikunto (2002:104) mengatakan bahwa apabila populasi kurang dari 100 orang, maka diambil seluruhnya. Namun bila jumlah populasinya lebih dari 100 orang, maka sampel diambil sebesar 10% - 15%, 20% - 25%, atau lebih. Bila populasi besar, dan peneliti tidak mungkin mempelajari semua yang ada pada populasi, misalnya karena keterbatasan dana, tenaga dan waktu maka peneliti dapat menggunakan sampel yang diambil dari populasi tersebut. Dalam penelitian ini penulis akan mengambil dari sejumlah pegawai/anggota yang berjumlah 20 di bagian Sitipol Polrestabes Bandung yang dijadikan sebagai sampel penelitian.Mengingat jenis penelitian ini bersifat eksploratif yaitu dengan mengajukan beberapa pertanyaan-pertanyaan yang diambil dari literatur COBIT 5 dan klausul ISO 27001.

B. Metode Pengumpulan Data

Dalam penelitian yang dilakukan di Polrestabes Bandung, dilakukan pengumpulan data yang bertujuan untuk mendapatkan informasi yang dibutuhkan
sebagai bahan penelitian. Jenis data yang dikumpulkan terbagi menjadi dua jenis
yaitu :

1. Data Primer
   Data primer dihimpun langsung dari tempat penelitian. Dalam penelitian ini
   data primer berupa hasil penyebaran kuisioner yang didistribusikan kepada
   bagian bagian tertentu yang sesuai dengan lingkup penelitian.
2. Data Sekunder
   Data sekunder adalah data yang digunakan untuk melengkapi data primer yang diperoleh dari responden, data sekunder diperoleh dari beberapa referensi seperti buku-buku peraturan-peraturan, laporan hasil penelitian, dokumen dan arsip dari Polrestabes Bandung yang berkaitan dengan penelitian. Untuk mendapatkan data sekunder dilakukan berbagai cara diantaranya dengan Studi dokumentasi. Dalam studi dokumentasi ini pengumpulan data dilakukan dengan cara mencari referensi dari berbagai media, seperti dokumen instansi, catatan kasus, laporan kerja, dan lain sebagainya yang terdapat di lingkungan ataupun di luar obyek penelitian. Selain itu juga menggunakan buku, jurnal ilmiah dan panduan COBIT 5 dan ISO 27001

C. Uji Validitas dan Reliabilitas

Interpretasi yang digunakan dalam menentukan validitas item, mengacu pada pendapatnya Masrun (1979) dalam Sugiyono (2006:148). Masrun menyatakan bahwa item yang mempunyai korelasi positif dengan kriterium (skor total) serta korelasi yang tinggi, menunjukkan bahwa item tersebut mempunyai validitas yang tinggi pula.

a. Uji Validitas
   Uji validitas dilakukan untuk mengukur suatu ketepatan. Pengujian dilakukan terhadap 20 responden. Jika didapatkan suatu instrumen yang valid maka instrumen tersebut pasti reliable, sebaliknya jika instrumen item yang reliable maka instrumen tersebut belum tentu bernilai valid.

$$r = \frac{N\,(\sum XY) - (\sum X)\,(\sum Y)}{\sqrt{[N\,\sum X^2 - (\sum X)^2][N\,\sum Y^2 - (\sum Y)^2]}}$$

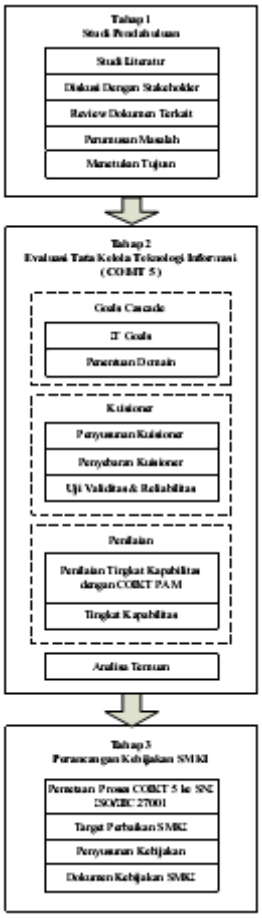
b. Uji Reliabilitas
   Uji Reliabilitas dapat dilakukan dengan uji Alpha Cronbach. Rumus Alpha Cronbach sebagai berikut :

$$a = \left(\frac{K}{K-1}\right)\left(\frac{S_r^2 - \sum S_i^2}{S_x^2}\right)$$

Dimana :
a : Koefisien reliabilitas Alpha Cronbach
K : Jumlah item pertanyaan yang diuji
$\sum S_i^2$: Jumlah varian skor item
S_x^2 : Varian skor-skor tes (seluruh item K)

D. Kerangka Penelitian

Untuk melakukan penelitian berdasarkan permasalahan yang telah diuraikan pada bab sebelumnya, maka berikut ini akan diuraikan tahapan-tahapan dalam penyusunan penelitian :. Urutan langkah-langkah penelitian penyelesaian masalah dapat dilihat pada Gambar 3.1 dibawah ini:



Gambar 3.1
Kerangka Penelitian

IV. HASIL PENELITIAN

A. Pemetaan Enterprise Goals (EG) ke IT Related Goals (ITRG

Polrestabes Bandung merupakan instansi pemerintah yang memiliki sistem komando dari atas kebawah, sehingga rencana strategis (Renstra) mengacu pada institusi renstra Kepolisian Negara Republik Indonesia (POLRI). Berikut ini adalah pemetaan EG (tujuan institusi) ke ITRG (tujuan IT pada institusi) yang diambil dari rencana strategis Kepolisian Negara Republik Indonesia. Tahun 2015 – 2019.

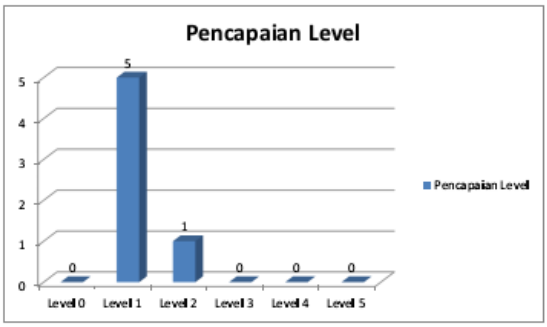
Tabel 4.1
Pemetaan Enterprise Goals (EG) ke IT Related Goals (ITRG)

ITRG	PROCESS
FINANCIAL	
ITRG 01 Alignment of IT and business strategy	APO01 Manage the IT Management Framework APO02 Manage Strategy APO07 Manage Human Resources
ITRG 02 IT compliance and support for business compliance with external laws and regulations	APO01 Manage the IT Management Framework APO12 Manage Risk APO13 Manage Security
ITRG 04 Managed IT-related business risk	APO12 Manage Risk APO13 Manage Security DSS01 Manage Operations DSS02 Manage Service Requests and Incidents DSS03 Manage Problems DSS04 Manage Continuity DSS05 Manage Security Services
ITRG 05 Realised benefits from IT-enabled investments and services portfolio	APO06 Manage Budget and Costs
ITRG 06 Transparency of IT costs, benefits and risk	APO06 Manage Budget and Costs APO12 Manage Risk
	APO13 Manage Security
CUSTOMER	
ITRG 07 Delivery of IT services in line with business requirements	APO02 Manage Strategy DSS01 Manage Operations DSS02 Manage Service Requests and Incidents DSS03 Manage Problems DSS04 Manage Continuity
INTERNAL	
ITRG 09 IT agility	APO01 Manage the IT Management Framework
ITRG 11 Optimisation of IT assets, resources and capabilities	APO01 Manage the IT Management Framework
ITRG 15 IT compliance with internal policies	APO01 Manage the IT Management Framework
ITRG 11 Optimisation of IT assets, resources and capabilities	APO07 Manage Human Resources
ITRG 13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	APO07 Manage Human Resources
ITRG 10 Security of information, processing infrastructure and applications	APO12 Manage Risk
ITRG 13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	APO12 Manage Risk
ITRG 10 Security of information, processing infrastructure and applications	APO13 Manage Security
ITRG 14 Availability of reliable and useful information for decision making	APO13 Manage Security
ITRG 11 Optimisation of IT assets, resources and capabilities	DSS01 Manage Operations
ITRG 11 Optimisation of IT assets, resources and capabilities	DSS03 Manage Problems
ITRG 14 Availability of reliable and useful information for decision making	DSS03 Manage Problems
ITRG 14 Availability of reliable and useful information for decision making	DSS04 Manage Continuity
ITRG 10 Security of information, processing infrastructure and applications	DSS05 Manage Security Services
LEARNING GROWTH	
ITRG 16 Competent and motivated business and IT personnel	APO01 Manage the IT Management Framework
ITRG 17 Knowledge, expertise and initiatives for business innovation	APO01 Manage the IT Management Framework
ITRG 17 Knowledge, expertise and initiatives for business innovation	APO02 Manage Strategy
ITRG 16 Competent and motivated business and IT personnel	APO07 Manage Human Resources
ITRG 17 Knowledge, expertise and initiatives for business innovation	APO07 Manage Human Resources

Dari hasil pemetaan diatas, maka disimpulkan bahwa domain yang akan gunakan sebagai bahan penilaian kapabilitas adalah APO01, APO12, APO13, DSS01, DSS03, DSS05.

B. Perhitungan Capability Level

Berdasarkan hasil perhitungan 6 proses COBIT yang dilakukan penelitian maka diperoleh hasil sebagai berikut :



Gambar 4.1
Capability Level

Berdasarkan hasil penilaian tingkat pencapaian kapabilitas didapatkan hasil level 1 sebanyak 5 proses dan level 2 hanya 1 proses, dari data tersebut kemudian dilakukan klasifikasi proses menggunakan tabel sebagai berikut :

Tabel 4.2
Pencapaian Level

Level	Management Practise	Target Level	Level saat ini	Selisih (Gap)
0	-			
1	APO12 - *Manage Risk*	3	1	2
	APO13 - *Manage Security*	3	1	2
	DSS01 - *Manage Operations*	3	1	2
	DSS03 - *Manage Problems*	3	1	2
	DSS05 - *Manage Security Services*	3	1	2
2	APO01 - *Manage the Management Framework for IT*	3	2	1
3	-			
4	-			
5	-			

Berdasarkan penilaian capability level langkah selanjutnya dilakukan perhitungan untuk mengetahui besarnya nilai rata-rata capability level yang dicapai teknologi informasi pada Polrestabes Bandung Rumus yang diterapkan adalah sebagai berikut :

$$capability\ level = \frac{(0 * y0) + (1 * y1) + (2 * y2) + (3 * y3) + (4 * y4) + (5 * y5)}{z}$$

Keterangan :
Yn (y0 ..... y5) = jumlah proses yang berada di level 2
Z = jumlah proses yang di evaluasi
Selanjutnya data pencapaian level dilakukan perhitungan sebagai berikut :

$$capability\ level = \frac{(0 * 0) + (1 * 5) + (2 * 1) + (3 * 0) + (4 * 0) + (5 * 0)}{6}$$

Maka nilai capability level adalah = 1,17 dibulatkan = 1. Berdasarkan hasil perhitungan maka dapat diambil suatu keputusan bahwa capability level Polrestabes Bandung berada di level 1.

Tabel 4.3
Hasil Kapabilitas Domain APO

Proses	*Align, Plan, Organize* (APO)			
	Management Preatise	Level	Target Level	Gap
APO01	Manage the Management Framework for IT	2	3	1
APO12	Manage Risk	1	3	2
APO13	Manage Security	1	3	2

Tabel 4.4
Hasil Kapabilitas Domain DSS

Proses	*Align, Plan, Organize* (APO)			
	Management Preatise	Level	Target Level	Gap
DSS01	Manage Operations	1	3	2
DSS03	Manage Problems	1	3	2
DSS05	Manage Security Services	1	3	2

Dari tabel di atas didapatkan nilai level 1 dan 2 dengan kondisi proses tersebut telah dikelola (managed) meskipun belum optimal secara menyeluruh dilakukan, untuk dapat mencapai level 2 dan level 3 maka langkah yang harus dilakukan antara lain melakukan solusi untuk memperbaiki kondisi tersebut .

C. Pemetaan Proses COBIT ke Klausul SNI ISO

Setelah melakukan proses perbaikan untuk peningkatan level pada proses domain di COBIT 5 dan memberikan rekomendasi kebijakan berkaitan dengan kondisi keamanan informasi yang masih belum optimal, maka langkah selanjutnya adalah merencanakan keamanan informasi menggunakan sistem manajemen keamanan informasi (SMKI) dengan melakukan terlebih dahulu proses mapping dari hasil kapibilitas COBIT 5 dengan Klausul SNI ISO 27001.

Tabel 4.5
Pemetaan COBIT 5 ke SNI ISO 27001

COBIT 5 Proses	Level Capability	ISO/IEC 27001 Control Objectives
APO01 : Manage the IT Management Framework	2	Tidak ada
APO12 : Manage Risk	2	A.8.3.3. Penghapusan hak akses A.11.1.1. Kebijakan kontrol akses A.11.2.3. Manajemen password pegawai A.11.2.4. Tinjauan terhadap hak akses pegawai dan pihak ketiga A.11.4.5 Pemisahan dalam jaringan A.12.1.1. Analisis dan spesifikasi persyaratan keamanan informasi
APO13 : Manage Security	1	A.11.4.1. Kebijakan penggunaan layanan jaringan A.11.4.3 Identifikasi peralatan di dalam jaringan A.11.5.2. Identifikasi dan otentifikasi user A.11.5.3. Manajemen password A.12.5.3. Pembatasan modifikasi piranti lunak A.12.5.5. Pengembangan piranti lunak yang menggandeng vendor.
DSS01 : Manage Operations	1	8.3.2 Pengembangan asset 11.1.1 Kebijakan kontrol akses 11.2.1 Registrasi pengguna 11.2.4 Tinjauan terhadap hak akses pegawai dan pihak ketiga 11.3.1 Penggunaan password 11.3.3 Kebijakan clear desk dan clear screen 11.4.6 Kontrol terhadap koneksi jaringan 11.5.4 Penggunaan utilitas sistem 11.5.5 Sesi time-out 11.5.6 Batasan waktu koneksi 11.7.1 Komunikasi dan terkomputerisasi yang bergerak
DSS03 : Manage Problems	1	11.6.1 Pembatasan akses informasi 11.7.2 Teleworking 12.2.2 Kontrol untuk pemrosesan internal 12.4.2 Perlindungan data pengujian sistem 12.5.4 Kelemahan informasi 12.6.1 Kontrol terhadap kelemahan secara teknis
DSS05 : Manage Security Services	1	11.2.2 Manajemen hak istimewa atau khusus 11.3.2 Peralatan pengguna yang tidak dijaga penggunaan password 11.4.2 Otentikasi pegawai atau pihak ketiga untuk melakukan koneksi keluar 11.4.4 Perlindungan remote diagnostic dan konfigurasi port 11.4.7 Kontrol terhadap routing jaringan 11.5.1 Prosedur log-on yang aman 11.6.2 Isolasi sistem yang sensitif 12.3.1 Kebijakan dalam penggunaan kontrol kriptografi 12.3.2 Manajemen kunci kriptografi 12.4.1 Kontrol operasional software 12.4.3 Kontrol akses ke sumber program 12.5.1 Prosedur perubahan kontrol

Dalam rangka memenuhi kebutuhan keamanan Informasi secara lebih efektif maka proses pengelolaan Keamanan Informasi harus dilakukan SMKI sedemikian rupa sehingga dapat memenuhi proses pematangan seperti yang diharapkan. Untuk dapat memenuhi hal tersebut maka diperlukan perancangan solusi atas berbagai permasalahan dan kelemahan yang menjadi kendala dalam pelaksanaan SMKI pada proses Klausul A.8, Klausul A.11 dan Klausul A.12. Adapun solusi ini akan dilakukan melalui tahapan berikut :

a. Beberapa hal penting dalam analisis yang dapat diperoleh adalah :
   1. Pada tahapan evaluasi tata kelola Kemananan Informasi dapat di identifikasi risiko dan perlu adanya kepedulian tentang dampak negatif sebagai suatu risiko.
   2. Pada penilaian tingkat kapabilitas (Cobit) telah diperoleh tingkat kematangan saat ini maupun yang diharapkan serta ditetapkannya strategi pencapaian kematangan yang diperlukan, yang dipandang efektif dalam rangka proses pematangan yang diharapkan.

b. Pendefinisian SMKI

Sesuai dengan strategi pencapaian kematangannya yang telah ditargetkan, maka usulan tindakan perbaikan untuk Pencapaian tingkat kematangan 2 dan tingkat kematangan 1. Perbaikan tingkat kematangan ini akan diawali dengan memprioritaskan kalusul dengan tingkat kematangan 1, sehingga jika semua kalusul tersebut telah mencapat tingkat kematangan 2, secara bersamaan proses pematangan akan digerakan agar tumbuh dari 2 menjadi 3.

D. Pemetaan SNI ISO/IEC 27001 terhadap Perancangan Kebijakan SMKI

Dalam merancang kebijakan SMKI terlebih dalulu dilakukan pemetaan mengenai proses manajemen terhadap SNI ISO/IEC 27001.

Tabel 4.6
Pemetaan Kebijakan Perancangan SMKI

Proses Manajemen	ISO/IEC 27001 Control Objectives
Manajemen Risiko	A.8.3.3. Penghapusan hak akses A.11.1.1. Kebijakan kontrol akses A.11.2.3. Manajemen password pegawai A.11.2.4. Tinjauan terhadap hak akses pegawai dan pihak ketiga A.11.4.5 Pemisahan dalam jaringan A.12.1.1. Analisis dan spesifikasi persyaratan keamanan informasi
Manajemen Keamanan	A.11.4.1. Kebijakan penggunaan layanan jaringan A.11.4.3 Identifikasi peralatan di dalam jaringan A.11.5.2. Identifikasi dan otentifikasi user A.11.5.3. Manajemen password A.12.5.3. Pembatasan modifikasi piranti lunak A.12.5.5. Pengembangan piranti lunak yang menggandeng vendor.
Manajemen Operasional	8.3.2 Pengembangan asset 11.1.1 Kebijakan kontrol akses 11.2.1 Registrasi pengguna 11.2.4 Tinjauan terhadap hak akses pegawai dan pihak ketiga 11.3.1 Penggunaan password 11.3.3 Kebijakan clear desk dan clear screen 11.4.6 Kontrol terhadap koneksi jaringan 11.5.4 Penggunaan utilitas sistem 11.5.5 Sesi time-out 11.5.6 Batasan waktu koneksi 11.7.1 Komunikasi dan terkomputerisasi yang Bergerak
Manajemen Masalah	11.6.1 Pembatasan akses informasi 11.7.2 Teleworking 12.2.2 Kontrol untuk pemrosesan internal 12.4.2 Perlindungan data pengujian sistem 12.5.4 Kelemahan informasi 12.6.1 Kontrol terhadap kelemahan secara teknis
Manajemen Layanan Keamanan	11.2.2 Manajemen hak istimewa atau khusus 11.3.2 Peralatan pengguna yang tidak dijaga
	penggunaan password 11.4.2 Otentikasi pegawai atau pihak ketiga untuk melakukan koneksi keluar 11.4.4 Perlindungan remote diagnostic dan konfigurasi port 11.4.7 Kontrol terhadap routing jaringan 11.5.1 Prosedur log-on yang aman 11.6.2 Isolasi sistem yang sensitif 12.3.1 Kebijakan dalam penggunaan kontrol kriptografi 12.3.2 Manajemen kunci kriptografi 12.4.1 Kontrol operasional software 12.4.3 Kontrol akses ke sumber program 12.5.1 Prosedur perubahan kontrol

V. KESIMPULAN

Berdasarkan hasil penjelasan pada bab sebelumnya, penulis dapat menarik kesimpulan diantaranya, sebagai berikut :

1. Pada dasarnya Polrestabes Bandung belum melakukan evaluasi tatakelola teknologi informasi. Seksi Teknologi Informasi Kepolisian (SITIPOL) yang memegang tanggung jawab terhadap Teknologi Infomasi di Polrestabes Bandung belum sepenuhnya melakukan pencatatan risiko yang terjadi secara detail ssetiap tahunnya, sehingga tidak diketahuai asset mana saja yang memiliki tingkat kerawanan dan ancaman yang tinggi.
2. Berdasrkan Hasil pengukuran dengan COBIT 5 PAM, Polrestabes Bandung memiliki tingkat kapabilitas (Capability level) tata kelola teknologi informasi di angka dua (2). Level ini ditunjukan berdasark an hasil analisis kuantitatif (kuisioner) yang dilakukan kepada 20 responden
3. Perancangan Kebijakan SMKI didasari oleh pemetaan tingkat kapabilitas dari proses COBIT 5 ke klausul pada SNI ISO/IEC 27001.

DAFTAR PUSTAKA

1. Alexander. 2008. “Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework”,
2. Andi Rifiandi. 2010. “Jurus Sukses Sertifikasi ISO 27001”
3. Erva Kurniawan. 2011. “Evaluasi Tata Kelola Teknologi Informasi Dengan Menggunakan Framework Cobit Studi Kasus: Pemerintah Provinsi Daerah Istimewa Yogyakarta”, Tesis MTI UGM.
4. ISACA. 2012.
5. ITGI. (2001). “Board Briefing on IT Governance”.
6. Jogiyanto, Prof.Dr. HM, MBA. 2005. “ Akt. Analisis dan Design” , Penerbit Andi, Yogyakarta.
7. Ministry of International Trade & Industry. , 1999. “Corporate approaches to IT Governance”.
8. Nurhayani. 2013. Jurnal “perancangan tata kelola teknologi informasi pada layanan akademik Di amik sigma palembang menggunakan analisis swot dan cobit”,
9. Richhardus Eko Indrajit. 2011 “Tata Kelola Teknologi Informasi”.
10. Riyanarto Sarno & Irsyat Iffano. 2013. “Sistem Manajemen Kemanan Informasi” Erlangga, Presentasi Training Cobit 5.
11. Razieh Sheikhpour, Nasser Modiri. 2012. “ An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, dipublikasikan di International Journal of Security and Its Applications “.
12. Selvi Amriani. 2012. Jurnal Sistem Informasi “ Analisis Resiko TI Berbasis” ISO 31000/310010
13. SNI ISO/IEC 27001. 2009. “Teknologi Informasi-Teknik Kemanan-Sistem manajemen kemanan informasi – Peryaratan”.
14. Sugiyono. 2013. “Memahami Penelitian Kualitatif Alfabeta. Bandung.
15. Van Grembergen. 2002. “ Introduction to the minitrack : IT Governance and its mechanism”.
16. Yohana Dewi Lulu W. 2013. Jurnal Teknik Elektro “Analisa Teori IT Governance menggunakan COBIT 5”.