Jurnal Maklumatika
Vol. 6, No. 1, Juli 2019 ISSN : 2407-5043

PENGEMBANGAN KEBIJAKAN KEAMANAN INFORMASI PADA JARINGAN TELEPON TETAP DAN STRATEGI PENERAPANNYA

Achmad Biowo
Program Studi Teknik Informatika, Universitas Indraprasta PGRI
Jl. Raya Tengah No 80 Kel. Gedong Jakarta Timur 13760
Email: achmad.birowo@gmail.com

Abstrak

Implementasi *Voice Over IP* (VoIP) yaitu percakapan melalui jaringan *Internet Protocol(IP),* telah banyak digunakan oleh operator telekomunikasi mapun perusahaan-perusahaan besar di dunia. Hal tersebut disebabkan kecenderungan semua *platform* jaringan menggunakan teknologi IP. Dengan semakin terbukanya *softswitch* (sentral telepon berbasis IP) dan *media gateway* terhadap jaringan IP Publik dan jaringan IP Pelanggan, serta kebutuhan remote ke perangkat-perangkat tersebut dengan menggunakan IP, maka hal tersebut meningkatkan resiko terhadap keamanan informasi. Operator telekomunikasi memerlukan suatu pengembangan atau penyempurnaan sistem keamanan informasi yang dapat menjamin *availability*, *confidentiality* dan *integrity* sehingga diharapkan target performansi perusahaan dan ekspektasi pelanggan dapat tercapai. Penelitian ini dilakukan untuk menyusun sistem keamanan informasi khususnya sub kebijakan keamanan informasi di Jaringan Telepon Tetap yang berbasis IP pada PT Indosat, Tbk serta strategi penerapannya. Penyusunan rancangan ini dilakukan dengan merujuk kepada kendali-kendali *The International Organization for Standarization(*ISO) 27001:2005, serta rujukan-rujukan lainnya termasuk materi kuliah Manajemen Resiko. Hasil dari penelitian diharapkan dapat memberikan masukan yang bermanfaat bagi Indosat atau bagi institusi akademis yang akan meneliti atau menerapkan sistem keamanan informasi pada jaringan telepon tetap .

***Kata kunci** : keamanan informasi, Voice Over IP, jaringan telepon tetap, ISO 27001, strategi penerapan*

I. PENDAHULUAN

1.1. Latar Belakang

Manajemen PT Indosat memutuskan bahwa permasalahan keamanan informasi merupakan hal yang penting sehingga dibentuk unit kerja khusus yang mengelola keamanan informasi. Salah satu keluarannya adalah membentuk *Information Security Policy* yang telah dijadikan kebijakan mulai bulan Desember 2006. Dalam menunjang keamanan informasi tersebut, salah satu aplikasi yang telah diterapkan adalah aplikasi *Identity Management* (IDM) yang berfungsi mengelola permohonan pengaktifan autentikasi dan otorisasi bagi karyawan permanen, karyawan non permanen serta rekanan.

Disamping keamanan informasi, manajemen meminta agar keamanan informasi di luar unit kerja Teknologi Informasi (TI), juga perlu dikembangkan. Bila memungkinkan diintegrasikan dengan IDM, sehingga IDM dapat dimanfaatkan pula untuk mengelola akses pengguna jaringan transmisi, jaringan telepon tetap sebagai contoh Sentral Lokal dan jaringan bergerak sebagai contoh MSC. Salah satu unit kerja di luar TI yang akan merupakan domain untuk penelitian ini adalah Grup Network Operation Maintenance (NOM) yang memiliki tugas melakukan pengoperasian dan pemeliharaan jaringan Indosat. Salah satu jaringan yang dioperasikan adalah Jaringan Telepon Tetap. Jenis Sentral yang termasuk jaringan telepon tetap adalah Sentral lokal, Sentral Sambungan Langsung Jarak Jauh Domestik dan Sentral untuk jasa Sambungan Internasional. Pengecualian untuk sentral lokal, pengoperasian dan pemeliharaan dilakukan oleh masing-masing regional. Dari masukan di atas mengenai pentingnya keamanan informasi, maka untuk meningkatkan sistem keamanan informasi pada jaringan telepon tetap, akan dilakukan penyusunan kebijakan keamanan informasi dan strategi penerapannya. Diharapkan dari hasil penelitian ini dijadikan masukan bagi Indosat atau institusi akadimisi lainnya yang berminat melakukan pengembangan sistem keamanan informasi khususnya pada jaringan telekomunikasi.

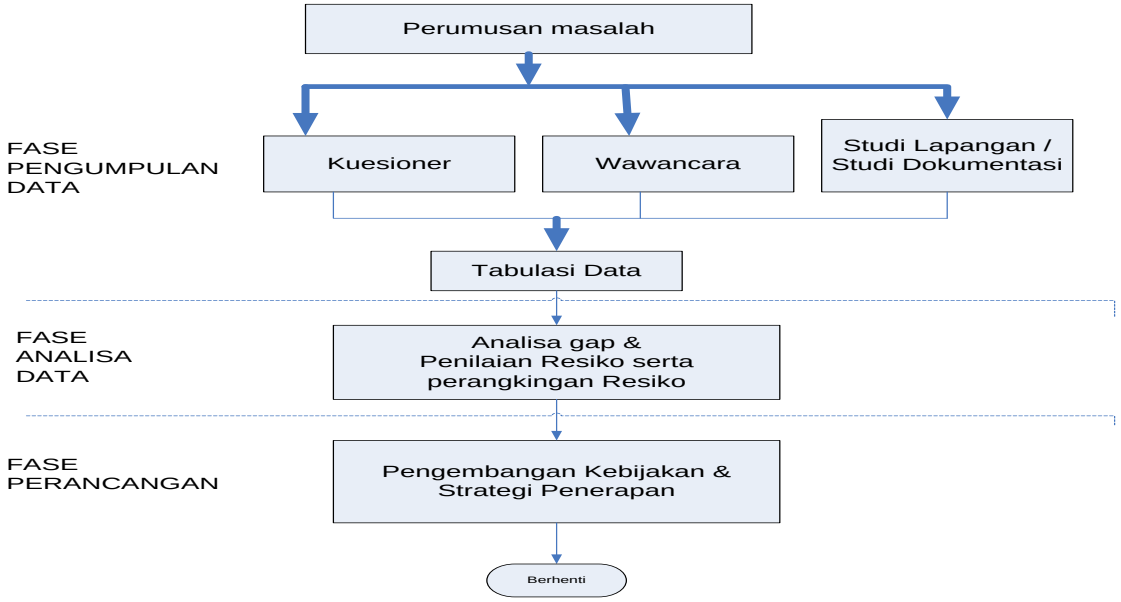
1.2. Rumusan Masalah

Adapun rumusan masalah dalam penelitian sebagai berikut :

1. Bagaimana bentuk kebijakan keamanan informasi untuk jaringan telepon tetap yang perlu diprioritaskan ?
2. Bagaimana strategi penerapannya ?

2. METODOLOGI PENELITIAN

Alur Pikir penelitian terdiri dari 4 tahap sebagai berikut (Gambar 1)



Gambar 1. Alur Pikir Penelitian

1. Merumuskan Masalah dan Studi Literatur
   Pada tahap pertama akan ditetapkan pokok permasalahan penelitian dan rumusan pertanyaan penelitian. Selanjutnya mempelajari teori-teori yang akan digunakan dalam penelitian, dimulai dengan penggalian materi dan referensi yang terkait khususnya penggalian materi mengenai kendali-kendali pada ISO 27001 dan ISO 27002 serta beberapa referensi lain terkait dengan pembuatan kebijakan keamanan informasi dan penilaian resiko.
2. Pengumpulan data
   Tahap ini dilakukan pengumpulan data berupa konfigurasi jaringan dan dokumen-dokumen keamanan informasi yang telah diterbitkan perusahaan mapun unit kerja terkait seperti Dokumen Kebijakan Keamanan Informasi dan Prosedur Operasional, serta kondisi dengan melihat secara langsung Operasional dari jaringan telepon tetap.
3. Analisa Data
   Pada tahap ini dilakukan Analisa Gap antara kebijakan dan implementasi pada jaringan tetap. Dari gap ini akan muncul potensi-potensi kelemahan keamanan informasi. Setelah itu pada tahap ini pula dilakukan penilaian resiko yang diawali dengan identifikasi aset, ancaman serta kelemahan. Setelah itu dilanjutkan dengan perangkingan resiko.
4. Pengembangan Kebijakan dan Strategi Penerapan
   Menurut ISO/IEC (2005:14) bahwa "*Controls objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process",* maka pada tahap ini dilakukan pemilihan kontrol kendali ISO 27001/27002 terutama untuk mitigasi resiko-resiko yang tinggi di jaringan telpon tetap, kemudian dilanjutkan penyusunan kebijakan keamanan informasi yang prioritas. Berdasarkan kebijakan keamanan informasi yang prioritas dikembangkan strategi penerapan yang secara rinci akan dibahas di bab terakhir. Urutan perencanaan seperti dijelaskan sebelumnya merujuk ke penjelasan Ivano

(2012:12) bahwa siklus perencanaan adalah *"Define Scope - Perform Gap Analysis - Perform Risk Assesment-Select Control- Establish set of Policies and Procedures".*

5. Kesimpulan
   Tahap ini adalah akan memberikan kesimpulan hasil penelitian dan saran penulis untuk perbaikan selanjutnya.

Metode Pengumpulan Data

Sub bab ini menjelaskan metoda pengumpulan data. Data yang diambil hanya meliputi konfigurasi jaringan saat ini, implementasi keamanan saat ini, serta kebijakan dan prosedur yang ada saat ini, serta wawancara.

Dalam pengumpulan data untuk keperluan penelitian, narasumber yang akan dihubungi adalah Staff dan Manager di Divisi *Core Network* dan Divisi *Technical Operation* Jabotabek yang terkait dengan konfigurasi, prosedur dan sistem keamanan pada sentral lokal, sentral SLJJ dan Sentral Gerbang International, Divisi Convergence Solution (marketing) serta divisi International Wholesale. Dilakukan pengumpulan informasi ke Divisi *IT Security* terkait apakah ada kebijakan yang terpusat terhadap seluruh perangkat di *Direktorat Technology*.

Data yang diperoleh dalam bentuk data kualitatif kemudian diinterpretasikan menjadi klasifikasi informasi tertentu pada tahapan analisa gap.

3. HASIL DAN PEMBAHASAN

Analisa Gap Kondisi Eksisting dengan Kendali ISO 27001

Berdasarkan kondisi keamanan informasi saat ini dilakukan analisa gap dengan kendali di ISO 27001. Pada Analisa gap ini, tidak dilakukan audit secara detil seperti yang dilakukan oleh internal audit karena bertujuan hanya untuk mengetahui kendali ISO 27001 yang belum diterapkan baik dari sisi kebijakan maupun implementasi. Dari hasil analisa gap, kemudian dikembangkan kelemahan-kelemahan keamanan informasi pada jaringan telepon tetap. Temuan kelemahan-kelemahan ini akan dijadikan masukan pada saat identifikasi resiko. Informasi yang diperoleh dari wawancara dan studi lapangan/dokumentasi, digolongkan menjadi 3 tingkatan sebagai berikut:

1. Kebijakan belum ada.
2. Ada kebijakan tetapi belum ada prosedur atau belum diimplementasikan
3. Ada prosedur atau standard, dan telah diimplementasikan

Untuk kasus telah dilakukan implementasi tetapi belum ada prosedur, maka akan dikelompokkan sebagai kebijakan belum ada. Pada analisa gap ini, semua domain dipilih tetapi untuk kendali, dipilih yang berkaitan dengan jaringan telepon tetap. Kendali yang dipilih biasa disebut dengan *Statement of Aplicability*(SOA). Dari 134 kendali, dipilih 119 kendali atau 89% dari seluruh kendali ISO 27001. Pertimbangan tidak rincinya penjelasan SOA, karena pada tahap ini difokuskan melakukan identifikasi kendali-kendali saat ini dan identifikasi kelemahan-kelemahan saat ini pada saat survei.

Pengklasifikasian terhadap suatu kendali masuk kategori 1, 2 dan 3, didasarkan atas dokmentasi yang dikumpulkan seperti Kebijakan Keamanan Informasi Indosat versi 2006, SOP pada jaringan telepon tetap serta beberapa nota dinas yang terkait kebijakan.

Berikut adalah hasil evaluasi kondisi eksisting terhadap ISO 27001 diklasifikan atas *Control Objective and Control* seperti dijelaskan dalam *ISO/IEC (2005:19).*

Tabel 1. Rekapitulasi *Compliance Gap* (2012)

No	ISO 27001 Control Domain	Type	Con-trol	SOA	Compliance				
				N	1	2	3	Kebijakan	Implementasi
1	Security policy	MC	2	2	1	1	0	50%	0%
2	Organization of information security	MC	11	11	5	4	2	55%	18%
3	Asset management	MC	5	5	2	1	2	60%	40%
4	Human resources security	MC	9	9	4	2	3	56%	33%
5	Physical and environmental security	PC	13	13	4	3	6	69%	46%
6	Communication and operational management	TC	33	30	11	10	9	58%	27%
7	Access control	TC	25	25	4	17	4	84%	16%
8	Systems development and maintenance	TC	16	11	1	8	2	63%	13%
9	Information security and incident management	MC	5	5	2	3	0	60%	0%
10	Business Continuity Plan	MC	5	5	3	2	0	40%	0%
11	Compliance	MC	10	3	1	2	0	20%	0%
			134	119	38	53	28	60%	21%

Keterangan:
Control : Jumlah Kendali di ISO 27001
SOA : Jumlah Kendali yang terkait dengan jaringan telepon tetap
1 : Jumlah Kendali yang belum ada kebijakan
2 : Jumlah Kendali yang telah ada kebijakan
3 : Jumlah Kendali yang telah diimpdlementasikan
Kebijakan : persentase dari (penjumlahan kolom '2' + kolom '3') dibandingkan kolom 'control'
Implementasi : persentasi kolom '3' dibandingkan kolom 'control'
MC : *Management Control* :
TC : *Technical Contro*l
PC : *Physical Control*

Beberapa kelemahan yang ditemukan pada analisa gap ini adalah

1. Perjanjian dengan pihak ketiga belum detil sesuai dengan ISO 27001.
2. Log-log akses ke perangkat jaringan telepon tetap belum dievaluasi secara rutin
3. Login ke perangkat masih diperbolehkan dengan menggunakan tool tanpa enkripsi yang baik
4. Untuk koneksi yang menggunakan *Session Border Controller*(SBC), saat ini belum dilakukan perekaman *IP Address* IP PBX Pelanggan untuk keperluan analisa fraud.

Identifikasi kelemahan pada analisa gap akan digunakan sebagai masukan pada pembahasan penilaian resiko.

Penilaian Resiko

Penilaian Resiko diawali dengan penyusunan Kriteria Pengukuran Kemungkinan (*Likehood*) dan kriteria Pengukuran Dampak (*Impact*).

Besar Resiko akan dihitung dari perkalian atas *Likehood* dan *Impact* dan setiap asset yang diidentifikasi akan dihitung nilai resikonya dan selanjutnya dilakukan perangkingan.

Kriteria Pengukuran Kemungkinan (*likelihood*)

Pengukuran *likelihood* diklasifikasikan menjadi 5 sebagai berikut mulai dari yang paling jarang hingga yang paling sering: *Rare , Unlikely, Possible, Likely dan Almost Certain*. Nilai kuantifikasi dari *likelihood* ini adalah mulai dari 1 sampai dengan 5.

Tabel 2. Nilai Kuantifikasi dari *Likehood*

JENIS ANCAMAN	SKALA *LIKELIHOOD*				
	Rare	*Unlikely*	*Possible*	*Likely*	*Almost Certain*
	1	2	3	4	5
Ancaman gangguan yang menyebabkan perangkat down atau salah satu fungsi terganggu baik karena bencana alam, kerusakan sistem maupun tindakan pengrusakan oleh seseorang.	>3 tahun atau peluang kejadian <20%	antara 1 - 3 tahun atau peluang kejadian antara 21% - 40%	antara 1 - 3 tahun atau peluang kejadian antara 41% - 60%	Mungkin terjadi dalam 1 tahun dengan peluang kejadian antara 61% - 80%	Sangat mungkin terjadi dalam 1 tahun atau peluang kejadian 81%-100%

Kriteria Pengukuran Dampak (*impact*)

Pengukuran dampak diklasifikasikan menjadi 5 mulai dari yang paling kecil dampaknya hingga yang terbesar dampaknya yaitu *insignificant, low, medium, high, critical*.

Tabel 3. Nilai Kuantifikasi dari Dampak

JENIS ANCAMAN		**SKALA DAMPAK**			
	Insignificant	***Low***	***Medium***	***High***	***Critical***
	Score : 1	***score :2-3***	***score: 4-6***	***score: 8-10***	***score: 12-14***
(D1) Dampak kerugian terhadap perkiraan revenue tahunan	Tidak menimbulkan Dampak berarti.	Kehilangan Net Income sampai dengan Rp 50 juta	Kehilangan Net Income sampai dengan Rp 100 juta	Kehilangan Net Income sampai dengan Rp 1 Milyar	Kehilangan Net Income lebih dari 1 milyar
(D2) Dampak terhadap reputasi dan hukum	Tidak menimbulkan dampak berarti	Keluhan via media komunikasi (telepon/email/ fax)	Reputasi buruk Indosat di mata pelanggan yang bersangkutan atau adanya surat peringatan/ complaint pelanggan Denda/restitusi dari pelanggan	Denda/restitusi karena SLA tidak terpenuhi oleh mayoritas pelanggan; Penghentian Kontrak Pelanggan	Publikasi buruk di media nasional (Berita, Surat Pembaca) atau Tindakan hukum melalui proses pengadilan atau penghentian kontrak pelanggan

Perhitungan Resiko

Perhitungan Resiko dilakukan per aset setelah itu nilai resiko diurutkan dari besar ke kecil seperti table berikut dibawah ini.

Tabel 4. Perhitungan Resiko

No	Aset	Resiko	*Threat* (Ancaman)	*Vulnerabilities*(Kelemahan)	Mitigasi Dampak	like hood	Impact	Nilai	risk	Priori ty
1	*OS & Database Softswitch sentral international dan SBC International*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers) {A1}*	*Vendor perangkat dapat masuk ke system 7x24 jam. Belum ada kontrak mengenai IS Security dng Vendor(V1). Belum ada monitoring log.*	*Backup konfigurasi*	*3*	*12*	*36*	*Extreme*	*10*
2	*OS & Database Softswitch sentral international dan SBC International*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers)*	*Belum ada policy agar OS tidak boleh melakukan login dari luar indosat, walaupun saat ini tidak OS yang login dari luar indosat. Belum ada monitoring log.*	*Backup konfigurasi*	*3*	*12*	*36*	*Extreme*	*10*
3	*OS & Database Softswitch sentral international dan SBC International*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers)*	*Telnet masih dibuka dari seluruh LAN (V3)*	*Backup konfigurasi*	*3*	*12*	*36*	*Extreme*	*10*

No	Aset	Resiko	*Threat* (Ancaman)	*Vulnerabilities*(Kelemahan)	Mitigasi Dampak	like hood	Impact	Nilai	risk	Priority
4	*OS & Database Konfigurasi sentral lokal dan SBC local*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers) {A1}*	*(=V1)Vendor perangkat dapat masuk ke system 7x24 jam*	*Backup konfigurasi*	*3*	*8*	*24*	*high*	*9*
5	*OS & Database Konfigurasi sentral lokal dan SBC local*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers) {A1}*	*(V2) Belum ada policy agar OS tidak boleh melakukan login dari luar indosat*	*Backup konfigurasi*	*3*	*8*	*24*	*high*	*9*
6	*OS & Database Konfigurasi sentral lokal dan SBC local*	*Database terhapus yang berakibat down(R1)*	*Unauthorized Users (disgruntled manage serive/vendor, hackers)*	*Telnet masih dibuka dari seluruh LAN (V3)*	*Backup konfigurasi*	*3*	*8*	*24*	*high*	*9*
7	*Username / Password pelanggan*	*Integrity*	*hacker (coba melakukan call dengan weak password)*	*masih menggunakan standar password. Prosedur aktifasi mulai dari sales sampai ke tim teknis masih belum secure*	*belum dibuka dari jaringan publik*	*3*	*8*	*24*	*high*	*8*
8	*OS & Database Softswitch sentral international dan SBC International*	*Down karena perangkat restart*	*Unauthorized User melakukan kesalahan command*	*Belum ada Monitoring dan review Log*	*Backup konfigurasi*	*3*	*8*	*24*	*high*	*7*
9	*OS & Database Konfigurasi sentral lokal dan SBC local*	*Down karena perangkat restart*	*Unauthorized User melakukan kesalahan command*	*Belum ada Monitoring dan review Log*	*Backup konfigurasi*	*3*	*6*	*18*	*high*	*7*
10	Softswitch Sentral International + SBC International	*down*	*power supply failure*	*belum dilakukan audit terhadap diversity power pada perangkat terpasang*	*perangkat memiliki main and backup power*	*2*	*8*	*16*	*high*	*7*

Pemilihan kendali

Sesuai dengan hasil penilaian resiko sebelumnya, yaitu terdapat resiko pada jaringan telpon tetap baik lokal maupun internasional dengan kategori *extreme*, *high* , *medium dan low*. Dilakukan pemilihan resiko dengan kategori *extreme* dan *high*, mengingat resiko *extreme* dan *high* tidak dapat diabaikan dalam waktu dekat. Jumlah aset yang memiliki resiko *extreme* dan *high* adalah 10, dimana setiap resiko akan dipilih kendali-kendali di ISO 27001 yang dapat memitigasi resiko tersebut. Hasil pemetaan *Vulnereabilities*(Kelemahan) dan kendali-kendali di ISO 27001 dapat dilihat pada Tabel 5.

Tabel 5. Pemilihan Kendali untuk Mitigasi

No	*Vulnerabilities* (Kelemahan)	*Risk*	*Priority*	*Select Control*
1	*Vendor* perangkat dapat masuk ke system 7x24 jam (karena status masih project). Belum ada kontrak mengenai *IS Security* dng *Vendor*(V1)	*Extreme*	*10*	*A.11.5 OS Access Control, A.11.4.2 User authentication for external connection, A.10.10.1 Audit logging,A.10.10.2 Monitoring system use, A.6.1.5 Confidentially agreements, A.6.2.1 Identification of risks, A.6.2.3 Addressing security in third party*
2	Belum ada policy agar OS tidak boleh melakukan login dari luar indosat, walaupun saat ini tidak OS yang login dari luar indosat. Hirarki dan matrik otoritas belum dirancang (V2)	*Extreme*	*10*	*A.11.5 OS Access Control, A.10.10.1 Audit logging, A.10.10.2 Monitoring System Use. A.11.4.2 User authentication for external connections, A.11.4.1 Policy on use of network services. A.6.2.1 Identification of risks, A.11.4.7 Network routing control*
3	*Telnet* masih dibuka dari seluruh *LAN* (V3)	*Extreme*	*10*	*A.10.10.4 Administrator and operator logs, A.11.4.2 User authentication for external connections*
4	(=V1)*Vendor* perangkat dapat masuk ke system 7x24 jam	*High*	*9*	*idem no 1*
5	(V2) Belum ada kebijakan agar OS tidak boleh melakukan login dari luar Indosat	*High*	*9*	*idem no 2*
6	*Telnet* masih dibuka dari seluruh *LAN* (V3)	*High*	*9*	*idem no 3*
7	Masih menggunakan standar *password*. Prosedur aktifasi mulai dari sales sampai ke tim teknis masih belum secure	*High*	*8*	*A.11.4.7 Network routing control*
8	Belum ada *Monitoring* dan *review Log*	*High*	*7*	*idem no 2*
9	Belum ada *Monitoring* dan *review Log*	*High*	*7*	*idem no 2*
10	belum dilakukan audit terhadap *diversity power* pada perangkat terpasang	*High*	*7*	*9.2.2 Supporting utilities*

Penyusunan Kebijakan Prioritas

Sesuai dengan pemilihan kendali yang dilakukan pada sub bab sebelumnya, selanjutnya dilakukan penyusunan kebijakan yang diambil dari kendali yang ada di ISO 27001.

Tidak seluruh isi dari setiap kendali akan dijadikan kebijakan untuk jaringan telepon tetap, tetapi standar yang relatif berhubungan yang diambil sebagai kebijakan keamanan informasi untuk jaringan telepon tetap. Terdapat 10 Kebijakan yang perlu diterapkan yang terkait dengan ancaman yang berisiko extreme dan high sebagai berikut:

Tabel 6. Daftar Kebijakan Prioritas

No	**Nama Kebijakan**	**Ancaman/ Resiko *)**
1	Kebijakan Pengendalian Akses Sistem Operasi (11.5)	1,2,4,5,8,9

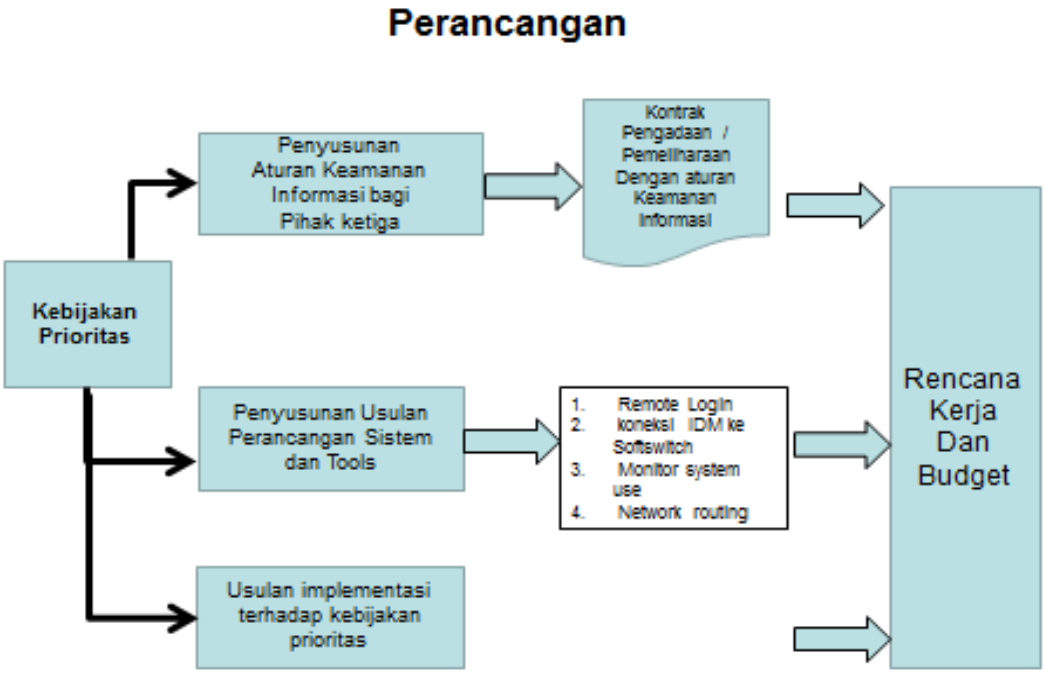
No	Nama Kebijakan	Ancaman/ Resiko *)
2	Kebijakan Autentikasi *User* untuk Koneksi Eksternal (A.11.4.2)	1,2,3,4,5,6
3	Kebijakan Pengauditan Log (A.10.10.1)	1,2,4,5,8,9
4	Kebijakan Pemantauan Penggunaan Sistem (A.10.10.2)	1,2,4,5,8,9
5	Kebijakan Perjanjian Konfidensial (A.6.1.5)	1,2 , 4,5
6	Kebijakan Identifikasi Resiko terkait dengan Pihak Ketiga (A.6.2.1)	1,2,4,5,8,9
7	Kebijakan *Addressing Security* pada Pihak Ketiga (A.6.2.3)	1,2,4,5
8	Kebijakan dalam Penggunaan Layanan Jaringan (A.11.4.1)	1,2,3,4,5,6
9	Pengendalian *Routing* Jaringan (A.11.4.7)	7
10	Sarana Penunjang (A.9.2.2)	10

Perancangan Sistem

Berdasarkan 10 kebijakan prioritas yang disusun sebelumnya, maka dilakukan perancangan yang meliputi 3 hal dengan pemetaan yang diuraikan pada tabel 7 dan alur perancangan yang dijelaskan pada gambar 2.

Tabel 7. Peta Kebijakan dan Rancangan/Rencana Implementasi

No	Kebijakan	Rancangan/Rencana Implementasi
1	Kebijakan Perjanjian Konfidensial , Kebijakan Identifikasi resiko terkait dengan pihak ketiga, Kebijakan *Addressing Security* pada pihak ketiga	Terkait dengan Aturan yaitu penyusunan aturan keamanan informasi bagi pihak ketiga dengan tujuan pihak ketiga dan karyawan berjangka akan lebih berhati-hati dalam melakukan pemeliharaan dan pengoperasian perangkat serta meminimalkan keinginan melakukan kecurangan dari pihak ketiga.
2	Kebijakan Pengendalian Akses Sistem Operasi, Kebijakan Autentikasi user untuk koneksi eksternal, Kebijakan Pengauditan Log, Kebijakan dalam penggunaan layanan jaringan, Kebijakan Pengendalian *Routing* Jaringan.	Terkait dengan rancangan sistem dan *tools* yaitu perancangan sistem dan *tools* yang bertujuan mempermudah melakukan pengendalian, dan mengurangi kemungkinan terjadinya serangan. Berapa rancangan atau standar teknologi yang diterapkan adalah a. Standar *remote login.* b. Implementasi IDM pada perangkat jaringan telepon tetap. Untuk implementasi ini dibutuhkan *API* antara Aplikasi IDM dan perangkat-perangkat jaringan telepon tetap seperti *softswitch, SBC, Media gateway* dan lain-lain. c. Perancangan aplikasi untuk pemantauan penggunaan sistem . d. *Routing* Jaringan yang diterapkan untuk pelanggan
3	Diluar aturan dan rancangan sistem yaitu untuk kasus yang belum diperoleh solusi dari *point* 1 dan *point* 2.	Audit terhadap sistem catu daya untuk perangkat sentral lokal dan sentral internasional.



Gambar 2. Rancangan dan Rencana Implementasi

Strategi Penerapan

Sebelum dilakukan pembahasan rencana kerja, dilakukan perhitungan berapa nilai kerugian (analisa dampak bisnis) bila terjadi *outage* atau bila terjadi percakapan ilegal. Tabel 8 menjelaskan nilai pendapatan dari jaringan telepon tetap lokal dan jaringan tetap internasional. Untuk jaringan internasional, *outage* total selama 1 jam berdampak kehilangan pendapatan sekitar Rp 150 juta sedangkan untuk Jartap Lokal sekitar Rp 11 juta. Dari aspek lain bahwa group NOM memiliki *Key Performance Indicator*(KPI) yaitu untuk Perangkat Sentral/*Core*, target *Continuity of Service* adalah 99.99% (52 menit dalam satu tahun) sehingga bila terjadi down lebih dari 52 menit (dalam setahun), maka target unit kerja tersebut tidak tercapai.

Rencana kerja untuk penyempurnaan keamanan informasi jaringan telepon tetap serta anggarannya adalah sebagai berikut dapat dilihat pada Tabel 8. Perkiraan kerugian disebabkan oleh percakapan ilegal dimana pelanggan tidak merasa menggunakan percakapan adalah sekitar Rp 50 juta per kejadian. Perhitungan tersebut berdasarkan histori kejadian *fraud* di jaringan telepon tetap.

Tabel 8. Program Kerja , Biaya dan Dampak Resiko

No	Kegiatan	Kebijakan	JENIS	Man Days	unit cost	Biaya (Rp)	Resiko	Nilai Kerugian	Nilai (Juta rupiah)
1	Penyusunan aturan keamanan informasi untuk pihak ketiga	A.6.1.5 dan A.6.2.1	-	22	500,000	11,000,000	Memanfaatkan *userid* untuk keperluan merestart atau shutdown perangkat	Rp 1 jam *down* = Rp 150 juta	150
2	Implementasi *standard Remote Login*	A.11.5 dan A.11.4.2	-	12	500,000	6,000,000	Memanfaatkan *userid* untuk keperluan merestart atau *shutdown*	RP 1 jam *down* = RP 150 juta	150

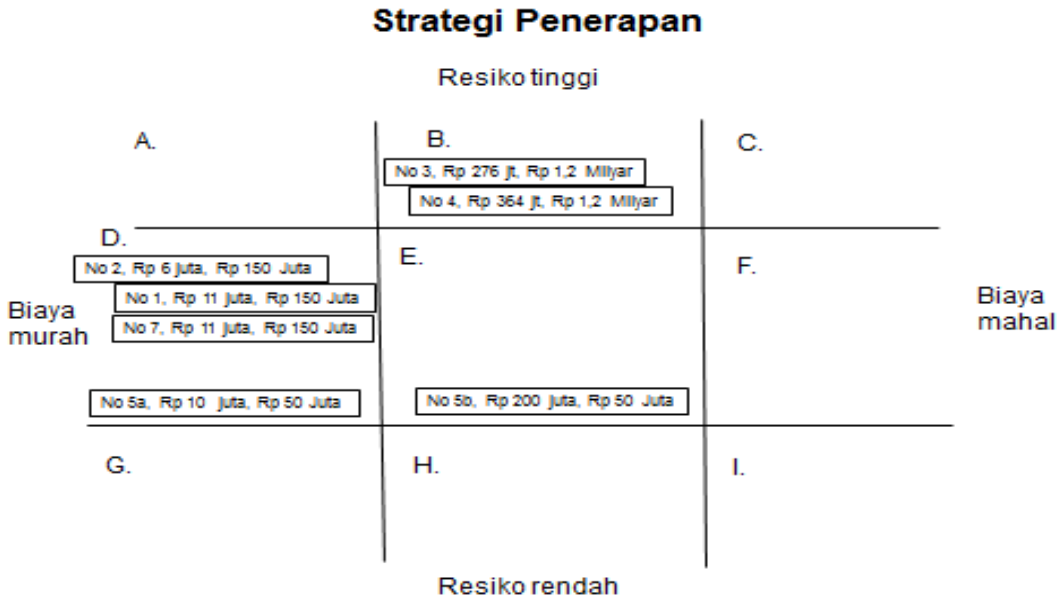
No	Kegiatan	Kebijakan	JENIS	Man Days	unit cost	Biaya (Rp)	Resiko	Nilai Kerugian	Nilai (Juta rupiah)
							*p*erangkat		
3	Pengembangan koneksi dari aplikasi IDM ke sentral lokal dan sentral gerbang international	A.11.5	Biaya programing + Lisensi *API* di *softswitch , Media gateway dan SBC*	138	2,000,000	276,000,000	Memanfaatkan *userid* untuk keperluan menghapus *database*	8 jam *Down* = Rp 1,2 milyar	1200
4	Pengembangan aplikasi pemantauan penggunaan sistem	10.10.1 dan 10.10.2	Biaya programing + Lisensi *API* di *softswitch , Media gateway dan SBC*	182	2,000,000	364,000,000	Memanfaatkan *userid* untuk keperluan menghapus *database*	8 jam *Down* = Rp 1,2 milyar	1200
5	Pengembangan *Network Routing (setup SBC)*	A.11.4.7 , A.11.4.3	Biaya setup SBC dan Metro	20	500,000	10,000,000	Percakapan *illegal*	Rp 50 juta	50
6	Pengembangan *Network Routing* (pengembangan Aplikasi)		Pengembangan Aplikasi dan *server* untuk log analys *CDR SBC*	40	2,000,000	200,000,000	Percakapan *illegal*	Rp 50 juta	50
7	Audit sistem Catu Daya untuk Sentral lokal dan Sentral International	A.9.2.2	-	22	500,000	11,000,000	Sistem restart pada saat gangguan catu daya	*Down* 1 jam Rp 150 juta	150
			TOTAL BIAYA			878,000,000			2950

Implementasi Program Kerja

Adapun untuk implementasi program kerja diusulkan diprioritaskan sesuai dengan matrik biaya dan kerugian seperti dipetakan pada gambar 3. Resiko tinggi, menengah dan rendah adalah relatif terhadap 10 resiko tertinggi yang telah dijelaskan sebelumnya. Ada 9 kuadran dari matrik ini, yaitu

1. kuadran A : biaya murah resiko tinggi
2. kuadran B : biaya menengah resiko tinggi
3. kuadran C : biaya tinggi resiko tinggi
4. kuadran D : biaya rendah resiko menengah
5. kuadran E : biaya menengah resiko menengah
6. kuadran F : biaya tinggi resiko menengah
7. kuadran G : biaya rendah resiko rendah
8. kuadran H : biaya menengah resiko rendah

9. kuadran I : biaya tinggi resiko rendah



Gambar 3. Pemetaan Program Kerja terhadap resiko dan biaya pengembangan

Dari pemetaan biaya dan kerugian masing-masing program kerja maka urutan implementasi dapat dilakukan sebagai berikut:

1. Kuadran B yang diimplementasikan terlebih dahulu karena hasil perhitungan resiko adalah yang tertinggi dengan program kerja
   a. Pengembangan interkoneksi IDM dengan perangkat jartap.
   b. Pengembangan aplikasi Pemantauan Penggunaan Sistem
2. Berikutnya Kuadran D dengan tiga program kerja yaitu
   a. Pembuatan aturan keamanan informasi bagi pihak ketiga
   b. Pembuatan standar remote login
   c. Audit terhadap sistem catu daya bagi perangkat jaringan tetap
   d. Implementasi *Routing* Jaringan *IP Private* bagi *IP PBX* Pelanggan
3. Yang terakhir Kuadran E, diusulkan tidak diprioritaskan mengingat antara resiko dan biaya yang dikeluarkan, lebih banyak biaya yang dikeluarkan.

4. SIMPULAN

Dari hasil evaluasi terhadap sistem keamanan informasi pada jaringan telepon tetap Indosat khususnya hasil kalkulasi resiko dan perankingannya, maka disimpulkan

1. Standar ISO 27001 dan ISO 27002 sangat bagus untuk dijadikan rujukan pengembangan kebijakan keamanan informasi pada suatu perusahaan
2. Domain-domain pada ISO 27001 yang masuk dalam penyusunan kebijakan prioritas yaitu domain *"communication and operational management*" , domain "*access control*" , domain "*Organization of Information Security*" dan domain "*Physical and Enviromental Security*".

Implementasi SBC Indosat sangat membantu terhadap ancaman dari luar, karena beberapa jenis ancaman dari VoIP khususnya *DDOS attack* dapat ditangani oleh SBC, sehingga resiko dari ancaman luar cenderung sudah minimal.

Penggunaan metode perhitungan analisa resiko yaitu dengan menghitung *likelihood* dan dampak, cukup membantu dalam menentukan besar resiko sehingga pengembangan kebijakan dapat lebih fokus terhadap resiko yang dianggap tinggi dan selanjutnya dapat dikembangkan menjadi strategi penerapan yang lebih akurat bagi penyempurnaan keamanan informasi jaringan telepon tetap.

Otomatisasi pembuatan userid yang disebut dalam makalah ini yaitu aplikasi IDM merupakan aplikasi yang wajib (*mandatory*) diterapkan pada suatu perusahaan besar, mengingat banyak karyawan berjangka dan *vendor* yang masuk ke dalam sistem operasi perangkat inti yang kesemuanya dapat menimbulkan kerawanan yang relatif tinggi.

Fitur *SBC* yang dapat memvalidasi percakapan berdasarkan *IP Address* sangat penting untuk mencegah *fraud*, karena validasi berdasarkan hanya *userid* dan *password* saja sangat tidak aman diterapkan

DAFTAR PUSTAKA

Aviandi, Ivano. 2012. *"Materi Kuliah Manajemen Resiko Keamanan Informasi – Topik Standard & Regulation dan Topik Risk Assessment"*. MTI Fasilkom Universitas Indonesia.

ISO/IEC. 2005. "*ISO 27001:2005 :Information technology-Security techniques -Information security management systems Requirements"*. International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).