PEMBUATAN RENCANA KEAMANAN INFORMASI BERDASARKAN ANALISIS DAN MITIGASI RISIKO TEKNOLOGI INFORMASI

Aan AlBone
Jurusan Teknik Informatika, Universitas Pasundan
Lengkong Besar No 68, Bandung, Indonesia
E-mail: aanalbone@yahoo.com

ABSTRAK: Sebuah rencana keamanan informasi terdiri atas strategi dan pembagian tanggungjawab, yang bertujuan utama untuk menurunkan risiko yang berpotensi menjadi ancaman terhadap operasional perusahaan. Jika penyusunan rencana keamanan tidak berdasarkan hasil analisis risiko, akan dapat menyebabkan lemahnya strategi dalam mengantisipasi ancaman gangguan dan serangan terhadap aset perusahaan. Lemahnya strategi tersebut, disebabkan oleh proses identifikasi kelemahan dan kerawanan teknologi informasi yang tidak dilakukan dengan baik. Sebaliknya dalam penyusunan rencana keamanan seharusnya didasari oleh hasil analisis dan mitigasi risiko teknologi informasi, agar strategi keamanan yang diusulkan dapat secara efektif menurunkan risiko yang telah diidentifikasi melalui analisis dan mitigasi risiko. Proses analisis risiko selain menghasilkan identifikasi risiko, juga memberikan rekomendasi kontrol keamanan yang sesuai dengan risiko yang akan diturunkan. Kontrol keamanan yang direkomendasikan pada analisis risiko, selanjutnya akan dinilai kembali dari aspek efektivitas dan efisiensi dalam menurunkan setiap risiko, pada proses mitigasi risiko, sehingga proses ini akan memberikan dasar yang kuat dalam menentukan rencana keamanan informasi yang menyeluruh, efektif dan efisien, karena didasarkan dengan prioritas implementasinya.

Kata kunci: Analisis risiko, Mitigasi risiko, Rencana Keamanan Informasi

***ABSTRACT**: An information security plan consists of strategies and shared responsibility, the main aim is to reduce the risk of a potential threat to the company's operations. If the security plan is not based on the results of risk analysis, can cause weakness in the strategy to anticipate the threat of disruption and attacks on corporate assets. Weak strategy, caused by the process of identifying weaknesses and vulnerabilities of information technology is not done properly. Instead of the security plan should be based on the results of analysis and information technology risk mitigation, so that the security of the proposed strategy can effectively reduce the risks identified through risk analysis and mitigation. The process of risk analysis in addition to producing the identification of risk, also providing recommendations appropriate security controls with the risk would be reduced. The recommended security controls on risk analysis, will then be evaluated from the aspects of effectiveness and efficiency in reducing any risk, the risk mitigation process, so that this process will provide a strong foundation in information security plan to determine an overall, effective and efficient, since it is based with the impelementasinya priority.*

***Keywords:** risk analysis, risk mitigation, Information Security Plan*

PENDAHULUAN

Tahapan dalam pembuatan rencana keamanan informasi dapat disusun berdasarkan gangguan yang pernah terjadi, lokasi penyimpanan aset informasi, atau pemilihan perangkat keamanan yang sesuai dengan dana perusahaan. Terkadang pula rencana keamanan dituliskan dengan format dan isi yang berbeda-beda, sehingga perlu dilakukan penelitian tentang bagaimana rencana keamanan informasi yang bukan saja secara efektif menurunkan risiko, juga secara efisien dalam implementasinya. Pertanyaan penelitian ini perlu diawali dengan pemahaman terhadap rencana keamanan informasi yang lengkap, dan dukungan hasil analisis risiko dan mitigasi.

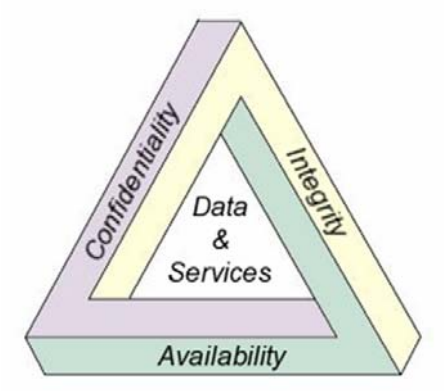
Rencana keamanan informasi (*information security planning*) merupakan susunan strategi yang diterapkan untuk mengurangi kelemahan dan menurunkan potensial ancaman dan risiko yang terkait dengan teknologi informasi yang berjalan, sehingga kemudian dapat dilakukan proses untuk meredakan risiko (*risk mitigation*), dan melakukan kontrol dan evaluasi [1].

Komponen dari rencana keamanan meliputi: kebijakan, standard dan prosedur keamanan informasi (*policy*), kontrol pengelolaan Sumber Daya Manusia (SDM) untuk keamanan informasi (*people*), dan kontrol teknologi keamanan informasi (*technology*). Kontrol yang dimaksud adalah langkah implementasi yang spesifik dan prosedural. Sedangkan yang menjadi kebutuhan penting rencana ini adalah permintaan level pengamanan yang diinginkan [1].

Rencana keamanan menjadi sangat penting, karena sebagai dasar dalam mengembangkan suatu

business continuity plan, yang berisi tentang langkah dan prosedur untuk selalu menjaga keberlangsungan bisnis yang dapat saja terganggu dengan gangguan yang mungkin dapat terjadi.

Pada dokumen *Information Security Plan Template*, yang dikelurkan oleh OTDA, keamanan informasi mengandung konsep lainnya, yaitu pengelolaan risiko, kebijakan (*policy*), prosedur (*procedure*), standar (*standards*), petunjuk (*guidelines*), klasifikasi informasi (*information classification*), operasi keamanan (*security operations*) dan *security awareness* [2].

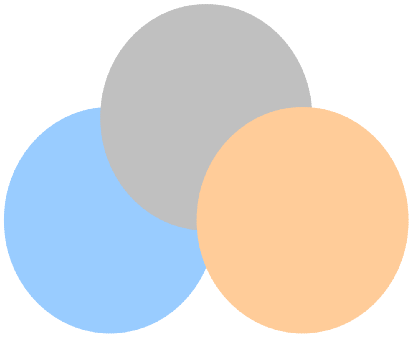


Gambar 1. CIA *triangle* [1]

Sesuai dengan Gambar 1, terdapat prinsip-prinsip penting dari sebuah rencana keamanan informasi (*information security*), yaitu: kerahasian (*confidentiality),* keutuhan data *(integrity)* dan ketersediaan (*availability)*. CIA adalah standar yang digunakan banyak pihak untuk mengukur keamanan sebuah sistem. Prinsip-prinsip keamanan informasi ialah sebagai berikut [6]:

- Kerahasiaan *(confidentiality),* yaitu membatasi akses informasi hanya bagi pengguna tertentu.
- Keutuhan data/informasi *(integrity),* yaitu taraf kepercayaan terhadap sebuah informasi. Dalam konsep ini tercakup *data integrity* dan *source integrity*.
- *Ketersediaan (availability),* yaitu ketersediaan, betul sekali. *Availability* yang dimaksud adalah ketersediaan sumber informasi.

Sebuah rencana keamanan harus dapat mengkombinasikan peran dari kebijakan, teknologi dan orang, dimana manusia (*people*), yang menjalankan proses membutuhkan dukungan kebijakan (*policy*), sebagai petunjuk untuk melakukannya, dan membutuhkan teknologi (*technology*) merupakan alat (*tools*), mekanisme atau fasilitas untuk melakukan proses [3]. Hubungan ketiganya dapat dilihat pada Gambar 2.



Gambar 2. *People, policy and technology model*

Sebuah rencana keamanan informasi, harus mampu menggambarkan langkah yang sistematis untuk menurunkan risiko, dengan cara mengimplementasikan kontrol keamanan berdasarkan sasarannya. Jenis kontrol berdasarkan sasarannya, sebagai berikut:

1. Kontrol administrasi *(administrative security)*,
2. Kontrol logik *(logical control)*, *intrusion detection*, dan anti-virus.
3. Kontrol fisik *(physical control)*

Kontrol keamanan tidak terlepas dari perlindungan terhadap aset informasi yang sensitif. Enterprise Information Technology Services (2001), dalam artikelnya yang berjudul "*Information Classification Standard*", menjelaskan bahwa informasi diklasifikasikan menjadi informasi sensitif dan kritikal. Informasi sensitif terkait dengan kerahasiaan (*confidentiality*) dan integritas data (*integrity*), sedangkan informasi kritikal terkait dengan ketersediaan data (*availability*) [3].

Berdasarkan uraian di atas, maka rencana keamanan akan berisi tentang penentuan kombinasi kontrol keamanan informasi yang digunakan, serta prioritas dalam melakukan implementasinya. Isi/ konten dasar pada dokumen rencana keamanan informasi (*information security plan*), antara lain:

1. Ancaman dan kelemahan, merupakan proses untuk mereview hasil tahapan penilaian risiko, dengan mengambil informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi.
2. Tujuan dan sasaran, merupakan proses menentukan target dan lingkup keamanan informasi yang ingin dicapai, sehingga dapat fokus pada aspek keamanan yang akan diselesaikan. Sasaran keamanan informasi menggambarkan spesifik hasil, kejadian atau manfaat yang ingin di capai sesuai dengan tujuan keamanan yang ditetapkan.
3. Aturan dan tanggungjawab, merupakan proses menyusun aturan dan penanggungjawab, yang mengatur kegiatan sebagai upaya untuk menurunkan risiko keamanan informasi yang bersumber dari ancaman dan kelemahan.

4. Strategi dan kontrol keamanan, merupakan proses untuk memberikan prioritas aksi yang akan dilakukan untuk mencapai tujuan dan sasaran keamanan informasi yang telah ditetapkan. Prioritas aksi tersebut sebagai pengaman untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi, dengan penentuan kontrol keamanan yang sesuai dengan tujuan dan sasaran yang diinginkan.

HASIL ANALISIS RISIKO

Analisis risiko pada akhirnya akan memberikan hasil identifikasi risiko, beserta rekomendasi kontrol keamanan yang terkait dengan upaya menurunkan risiko terserbut. Tahapan tersebut dinamakan rekomendasi kontrol.

Control recommendation akan menjadi hasil dari proses *risk assessment* dan akan menjadi input bagi proses *risk mitigation*, serta menjadi rekomendasi prosedur dan teknik dalam perencanaan keamaan informasi yang diimplementasikan ke depan.

Adapun rekomendasi yang dihasilkan dari atau analisis risiko, sebagai berikut:

- Risiko yang terkategori pada level "*Low*", dengan rangking 1 sampai 5, bernilai risiko rendah, sehingga yang dapat diterima.
- Risiko yang terkategori pada level "*Medium*", dengan ranking 6 sampai 10 bernilai menengah, dengan rekomendasi risiko tidak dapat diterima, sehingga risiko tersebut harus dihilangkan, dikurangi atau dipindahkan.
- Risiko yang terkategori pada level "*High*", dengan ranking 12 sampai 16 bernilai tinggi, dengan rekomendasi risiko tidak dapat diterima, sehingga risiko tersebut harus dihilangkan, dikurangi atau dipindahkan.

Tabel rekomendasi kontrol akan menjadi hasil dari tahap analisis risiko, yang selanjutnya menjadi input bagi tahap *risk mitigation*, tahap evaluasi, tahap analisis *cost-benefit* dan *cost effectiveness* terhadap kontrol keamanan yang direkomendasikan, dan pada

Tabel 1. Identifikasi risiko

No	Risk	Ranking	Risk Level	Recommended Control
1	Risiko kehilangan keamanan informasi (confidentiality, integrity, availability), jika informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka.	16	H	**Preventive:** Kebijakan dan prosedur (ADM) **Detective:** Pelabelan informasi sensitif (ADM)
2	Risiko terhentinya bisnis perusahaan, karena tidak memiliki rencana penanggulangan bencana, sehingga ketika terjadi bencana tidak mampu mempertahankan dukungan TI terhadap jalannya bisnis, secara sistematis	16	H	**Preventive:** Kebijakan dan prosedur (ADM) **Detective:** Kebijakan dan prosedur (ADM)
3	Petir di lokasi tersebut, intensitasnya cukup besar, sedang penangkalnya belum mampu meredamnya, disebabkan tidak memiliki grounded yang baik, sehingga berpotensi merusak dan membakar server dan perangkat jaringan.	16	H	**Preventive:** Kebijakan dan prosedur (ADM), Anti petir dan grounded (PHY) **Detective:** Kebijakan dan prosedur (ADM)
4	Risiko hilangnya data master dan backup berpotensi terjadi, jika ruang DRC berada pada ruang yang sama dengan ruang data center atau server yang saat mengalami bencana.	16	H	**Preventive:** Kebijakan dan prosedur (ADM), Penyimpanan Backup di tempat aman (PHY) **Detective:** Kebijakan dan prosedur (ADM)
5	Risiko penggunaan sistem operasi yang rentan dengan gangguan virus, tanpa didukung oleh perangkat antivirus yang cukup handal, berpotensi menimbulkan kerusakan file, dan kehilangan data.	16	H	**Preventive:** Pelatihan security awareness (ADM), scanning terhadap virus (TECH) **Detective:** Pelatihan security wwareness (ADM), violation reports (TECH)
6	Firewall diletakkan di sisi luar DMZ terhadap jaringan luas internet, dan tidak memiliki firewall lainnya disisi dalam DMZ terhadap jaringan lokal internal, sehingga berpotensi server menjadi terbuka dari serangan yang berasal dari jaringan internal.	12	H	**Preventive:** Kebijakan dan prosedur (ADM), firewall (PHY) **Detective:** kebijakan dan prosedur (ADM), Intrussion Detection System (TECH)
7	File system backup gagal saat direstore, maka berpotensi jika terjadi kehilangan data pada sistem utama, maka hasil backup tidak dapat direstore, sehingga harus meng-entry ulang berdasarkan form manual	12	H	**Preventive:** Kebijakan dan prosedur (ADM), Penyimpanan Backup di tempat aman (PHY) **Detective:** Sharing Responsibilities (ADM)

Tabel 2. Penilaian investasi

No	Kontrol		IIi	Pi	pi	Rank Prioritas
1	Kebijakan dan prosedur	Investasi 1	3814697265625.00000000000	357917.51085683000000000000	0.96	0.1933
2	Labelling of sensitive material	Investasi 12	18310546875.00000000000	1718.00405211278000000000	1.48	0.1459
3	Penyimpanan backup data pada tempat aman	Investasi 9	10546875.00000000000	0.98957033401696300000	1.00	0.0985
4	Pemeriksaan latar belakang	Investasi 6	98415.00000000000	0.00923387870077908000	0.78	0.0771
5	Perjanjian kerja	Investasi 10	11691.70200000000	0.00109698478965256000	0.70	0.0689
6	Pelatihan security awareness	Investasi 11	714.49290000000	0.00006703795936765620	0.60	0.0595
7	Sharing responsibilities	Investasi 3	218.31727500000	0.00002048382091789490	0.57	0.0559
8	Job rotation	Investasi 7	111.18009375000	0.00001043157546744650	0.55	0.0539
9	Increased supervisions	Investasi 13	7.41200625000	0.00000069543836449643	0.47	0.0468
10	Scanning terhadap virus	Investasi 16	1.63350000000	0.00000015326465333255	0.44	0.0432
11	Pemasangan anti petir dan ground	Investasi 18	0.00435600000	0.00000000040870574222	0.32	0.0316
12	Pemasangan firewall	Investasi 4	0.00025615894	0.00000000002403434988	0.28	0.0272
13	Intrussion Detection System	Investasi 2	0.00001149984	0.00000000000107898316	0.23	0.0231
14	Enkripsi	Investasi 16	0.00000009837	0.00000000000000922919	0.18	0.0180
15	Pembatasan fungsi dan informasi	Investasi 8	0.00000005962	0.00000000000000559345	0.18	0.0175
16	Penggunaan call back system	Investasi 6	0.00000000656	0.00000000000000061528	0.16	0.0156
17	Violation report	Investasi 14	0.00000000013	0.00000000000000001228	0.13	0.0127
18	Kebijakan dan prosedur	Investasi 17	0.00000000002	0.00000000000000000151	0.12	0.0114
			10658034.74239880000		10.14	1.0000

akhirnya akan dipilih. Pembahasan tentang tahap proses mitigasi dijelaskan pada bagian selanjutnya.

HASIL MITIGASI RISIKO

Proses mitigasi risiko merupakan upaya dalam menilai kontrol keamanan yang secara efektif dan efisien dapat menurunkan risiko teknologi informasi yang berpotensi terjadi. Tahapan pada mitigasi risiko antara lain adalah tahap analisis *effectiveness-cost* dan *cost-benefit analysis*. Pada tahap analisis *effectiveness-cost* kontrol keamanan akan dilakukan berdasarkan tahapan, sebagai berikut:

1. Melakukan identifikasi investasi dalam rangka implementasi kontrol keamanan yang telah direkomendasikan pada tahapan sebelumnya
2. Menghitung nilai prioritas, setiap investasi
3. Menentukan rangking prioritas investasi.

Tahap pertama ialah mengidentifikasi investasi dalam rangka implementasi kontrol keamanan, yang telah direkomendasikan.

Tahap kedua ialah menghitung nilai prioritas, dengan membandingkan efektivitas antar kontrol keamanan satu dengan lainnya, berdasarkan kemampuannya untuk mencapai tiga aspek keamanan informasi, yaitu: *confidentiality*, *integrity* dan availability. Adapun hasil dari identifikasi dan perbandingan seperti pada Tabel 2.

Tabel 2 menjelaskan ranking prioritas dari kontrol keamanan yang direkomendasikan. Data ini diharapkan dapat menjadi bahan pertimbangan dalam perencanaan keamanan informasi, sehingga dapat diketahui prioritas impelementasi kontrol agar dapat efektif dalam mencapai tujuan dan sasaran keamanan informasi.

Berdasarkan hasil dari *cost-benefit analysis*, pihak manajemen menentukan beberapa rekomendasi yang memiliki *cost-effectiveness* untuk mampu mengurangi dan menghilangkan risiko, maka rekomendasi kontrol yang dipilih untuk digunakan.

Pemilihan kontrol telah menyajikan hasil evaluasi, yang menyatakan bahwa seluruh kontrol telah sesuai dengan kerawanan/kelemahan yang akan dikurangi dan mampu menurunkan risiko di bawah maksimum risiko. Sedangkan analisis *cost-benefit*, yang menyatakan bahwa delapan belas kontrol yang direkomendasikan dapat mengurangi minimum resiko dengan biaya implementasi yang lebih kecil dibanding biaya (nilai risiko) jika tidak dimplementasi.

Analisis *cost effectiveness* memberikan prioritas dalam mengimplementasikan kontrol-kontrol tersebut, berdasarkan efektvitasnya dalam mencapai tujuan keamanan informasi (*confidentiality, integrity, dan availability*). Berdasarkan hasil evaluasi dan analisis, dapat disimpulkan bahwa delapan belas kontrol dipilih untuk diimplementasikan.

Tindakan selanjutnya setelah rekomendasi kontrol dipilih untuk diimplementasikan ialah menugaskan orang dengan deskripsi tugas tertentu, sebagai orang yang bertanggungjawab pada pengendalian perangkat untuk mengurangi dan menghilangkan risiko. Rencana tersebut berisi informasi hasil-hasil tahapan *risk mitigation* sebelumnya, yaitu antara lain:

a. Pilihan kontrol (*selected planned control*)
b. Prioritas aksi (*prioritize action*)
c. Kebutuhan sumber daya untuk implementasi kontrol (*required resources for implementing the selected planned control*)

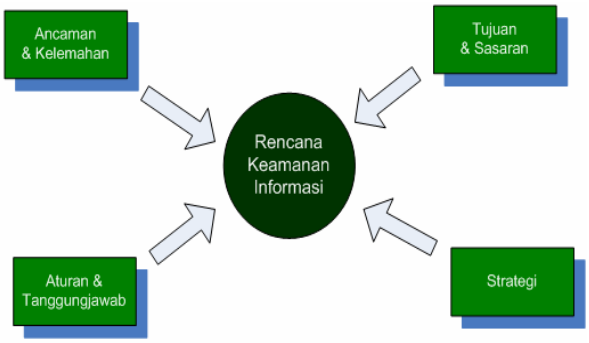
d. Penugasan personil yang bertanggungjawab (*list of responsible team and staff*)

Kontrol keamanan yang telah ditelaah, dipilih berdasarkan proses evaluasi, analisis *cost-benefit* dan *cost-effectiveness*, pada Tabel 2 dijelaskan kebutuhan sumber daya yang harus dimiliki, serta tim implementtator dari setiap kontrol keamanan, sehingga diharapkan dapat memberikan gambaran terhadap proses perencanaan keamanan informasi. Proses perencanaan keamanan informasi dijelaskan pada bagian selanjutnya.

RENCANA KEAMANAN TEKNOLOGI INFORMASI

Rencana keamanan informasi perusahaan, menyajikan tujuan, sasasan dan rencana dari kegiatan untuk mencapai keamanan sumber daya kritikal untuk melindungi informasi. Rencana keamanan merupakan hal yang strategis, yang harus dibangun dengan didahului melakukan penilaian risiko, dan mitigasi risiko [5].

Rencana keamanan informasi terdiri dari empat hal penting yaitu informasi ancaman dan kelemahan, aturan dan tanggung jawab, tujuan dan sasaran, dan strategi (Gambar 3).



Gambar 3. Rencana Keamanan Informasi

Ancaman dan kelemahan memberikan informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi jika terjadi dengan memanfaatkan potensi kegagalan atau kelemahan yang dimiliki oleh perusahaan. Perlu diketahui sumber ancaman dan kelemahan tersebut. Selanjutnya perlu ditemukan kontrol untuk menurunkan risiko dari ancaman dan kelemahan tersebut, serta priotitas penyelesaiannya.

Aturan dan tanggungjawab akan menunjukkan terdapatnya tata kelola keamanan informasi yang baik, dengan pengelolaan kontrol keamanan yang telah diusulkan. Aturan yang jelas akan sangat menentukan keberhasilan penerapan kotrol keamanan

Tabel 3. Kerawanan dan Ancaman

No	Vulnerability	Threat	C	I	A	Risk
1	Informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka	Informasi yang akan keluar dari perusahaan, harus terklasifikasi dan dilabelkan berdasarkan sensitifitas, jika tidak, maka informasi tersebut menjadi tidak diproteksi secara baik, menyebabkan hilangnya kerahasiaan informasi	√	√	√	H
2	Tidak memiliki rencana dalam penanggulangan bencana, sehingga tidak ada jaminan bahwa bisnis dapat berjalan secara cepat, setelah terjadi bencana.	Jika terjadi bencana, tidak memiliki alternative cara agar bisnis dapat terus berjalan, sehingga yang terjadi bisnis terhenti dan perusahaan mengalami kerugian.			√	H
3	Petir dilokasi tersebut, intensitasnya cukup besar, dan peralatan penangkal petir (anti petir dan grounding) belum mampu meredamnya	Server terancam rusak dan terbakar, disebabkan terkena petir.			√	H
4	Perangkat DRC yang masih berada pada ruang yang sama dengan data center dan server saat terjadi bencana	Jika terjadi bencana pada ruang server dan data center, maka DRC dan file backup mengalami bencana yang sama sehingga tidak mampu mengembalikan informasi dan sistem beroperasi kembali.			√	H
5	Sistem operasi yang rentan dengan gangguan virus dan meningkatnya penyebaran virus melalui email, tanpa didukung oleh perangkat antivirus yang cukup handal, dapat menimbulkan kerusakan file, dan kehilangan data.	Sistem operasi yang rentan dengan penyebaran virus, dapat berpotensi merusak informasi dan mengganggu jaringan komputer perusahaan.			√	H
6	Penggunaan firewall hanya pada sisi luar DMZ saja, berpotensi terbukanya wilayah server dari gangguan yang berasal dari dalam jaringan (local), karena area dalam DMZ tidak dilindungi firewall	Penyusupan dan gangguan yang berasal dari jaringan local dapat langsung masuk ke area DMZ dimana server berada, dan mengakses informasi dan system yang sensitive dan kritikal.	√	√	√	H

sebagai upaya untuk menurunkan risiko dari terjadinya gangguan yang bersumber dari ancaman dan kelemahan

Tujuan dan sasaran akan menentukan target dan lingkup keamanan informasi yang ingin dicapai, sehingga dapat fokus pada aspek keamanan yang akan diselesaikan. Sasaran keamanan informasi menggambarkan spesifik hasil, kejadian atau manfaat yang ingin dicapai sesuai dengan tujuan keamanan yang ditetapkan.

Strategi akan memberikan prioritas aksi yang dilakukan untuk mencapai tujuan dan sasaran keamanan informasi yang telah ditetapkan. Prioritas aksi tersebut sebagai pengaman untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi.

Ancaman dan Kerawanan

Ancaman dan kerawanan/kelemahan dapat menggambarkan risiko yang berpotensi diterima oleh perusahaan, berdasarkan aset-aset TI yang dinilai pada tahap penilaian risiko (*risk assessment*), maka dapat dihasilkan informasi kerawanan/kelemahan dan ancaman.

Menurut Peter Mell, dalam NIST *Standard* kesesuaian (*compatibility*) berarti kontrol yang direkomendasikan harus sesuai dengan kerawanan/ kelemahan (*vulnerability*) yang teridentifikasi, yang akan dihilangkan atau dikurangi. Sedangkan efektivitas kontrol keamanan yang direkomendasikan, bergantung dari kemampuannya dalam menurunkan risiko atau dampak yang ditimbulkan akibat kerawanan/kelemahan, sehingga dapat diketahui tingkat perlindungannya terhadap aset yang dimiliki perusahaan [6].

Aturan dan Tanggungjawab

Keamanan informasi tidak hanya terkait dengan masalah teknikal, tetapi juga harus didukung oleh aturan dan tanggungjawab yang dikeluarkan oleh organisasi, berupa tata kelola keamanan informasi (*information security governance*).

William Conner (2004) menjelaskan bahwa tata kelola keamanan informasi merupakan salah satu bagian dari konsep tata kelola organisasi yang baik (*good organization governance*), yang terdiri atas sekumpulan kebijakan dan kontrol internal perusahaan yang terkoordinasi dan terkelola [1, 2].

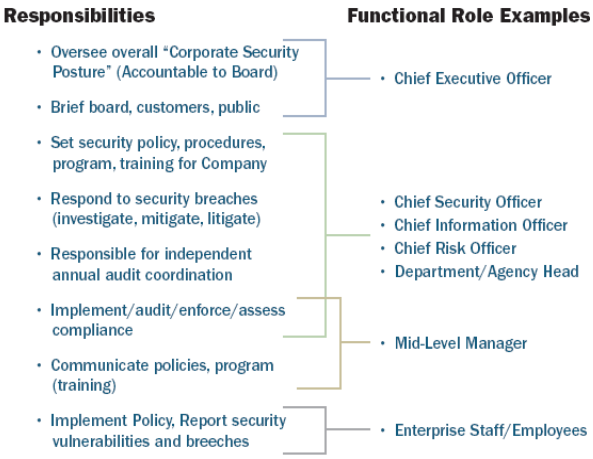
Dalam konsep tata kelola keamanan informasi, disampaikan bahwa terdapat kumpulan tanggungjawab dan aturan fungsional. Kumpulan tanggung jawab pada keamanan informasi di perusahaan, sebagai berikut:

- Bertanggungjawab mengelola secara keseluruhan berjalannya keamanan informasi perusahaan.
- Bertanggungjawab membuat laporan dan penjelasan kepada konsumen dan umum.
- Bertanggungjawab merancang kebijakan keamanan, prosedur, program dan pelatiahan keamanan informasi.
- Bertanggungjawab melakukan respon terhadap kejadian/insiden keamanan informasi dengan melakukan investigasi, mitigasi, dan penuntutan.
- Bertanggungjawab melakukan respon terhadap laporan hasil audit mengenai keamanan informasi.
- Bertanggungjawab melakukan audit, penilaian kesesuaian dan kebutuhan terhadap kontrol keamanan.
- Bertanggungjawab mengkomunikasikan dan mensosialisasikan kebijakan, program dan pelatihan kepada seluruh karyawan terkait keamanan informasi.
- Bertanggungjawab mengimplementasikan dan melaksanakan seluruh kebijakan, prosedur dan program keamanan informasi, serta melaporkan jika ditemukan kerawanan/kelemahan keamanan.

Adapun aturan fungsional pada tata kelola keamanan informasi, ialah:

- Chief Executive Officer (CEO)
- Chief Security Officer (CSO), atau Chief Information Officer (CIO), atau Chief Risk Officer (CRO), atau Departemen/Agency Head (DH)
- Mid-Level manager
- Staf atau karyawan

Berdasarkan kumpulan tanggungjawab dan aturan fungsional, maka dapat dikelompokkan seperti pada Gambar 4.



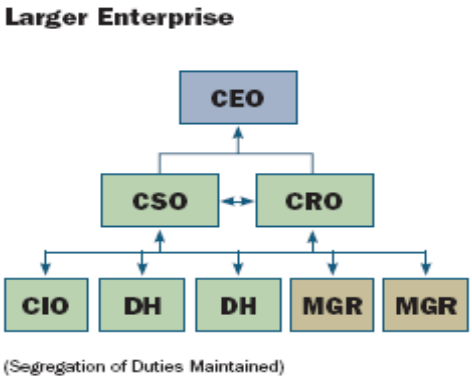
Gambar 4. Tanggungjawab dan aturan fungsional

Tanggungjawab dan aturan fungsional sangat terkait dengan struktur organisasi yang berlaku di organisasi tersebut, sehingga perlu untuk menampilkan

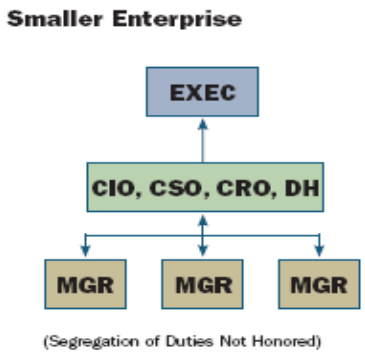
rekomendasi struktur organisasi pada tata kelola keamanan informasi perusahaan, seperti pada Gambar 5 dan Gambar 6.

Kedua struktur organisasi yang direkomendasikan oleh konsep tata kelola keamanan informasi, selanjutnya perlu melakukan analisis terhadap struktur organisasi perusahaan.

Struktur organisasi perusahaan meletakkan Divisi yang terkait dengan pengelolaan SI dan TI pada level ketiga dari pimpinan puncak, sehingga pengambilan keputusan dan pemberian pertimbangan dalam penetapan kebijakan menjadi tidak memiliki pengaruh besar.



Gambar 5. Rekomendasi Struktur Organiasi Keamanan Informasi (Larger)



Gambar 6. Rekomendasi Struktur Organisasi Keamanan Informasi (Smaller)

Berdasarkan pertimbangan di atas, maka direkomendasikan perubahan secara bertahap struktur organisasi perusahaan, yang mengarah pada tata kelola TI yang baik (IT *good governance*) dan tata kelola keamanan informasi yang baik (*good informatioan security governance*) yang semua itu, mengacu pada konsep besar yaitu tata kelola perusahaan yang baik (*good corporate governance*).

Tujuan dan Sasaran

Tujuan dari keamanan informasi perusahaan ialah meningkatkan kemampuan dalam mencegah, melindungi, merespon dan mengembalikan ke kondisi aman dari kejadian gangguan keamanan. Sasaran strategis ialah hal yang spesifik dalam membantu pencapaian tujuan dari keamanan informasi yang ditetapkan pada sebuah rencana keamanan.

Keberhasilan dalam mencapai tujuan, akan ditentukan oleh sasaran-sasaran yang mampu dipenuhi. Adapun penjelasan tentang setiap sasaran dibahas dalam bagian selanjutnya.

Sasaran pertama dari rencana keamanan informasi ialah dapat menentukan kebijakan yang dibutuhkan dalam mendukung implementasi keamanan informasi. Jika sasaran dapat dicapai, maka akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Kebijakan dan Prosedur klasifikasi informasi.
- Kebijakan dan Prosedur dekstop.
- Kebijakan dan Prosedur pencatatan kejadian gangguan keamanan TI.
- Kebijakan dan Prosedur Ruang DRC.
- Kebijakan dan Prosedur BCP dan DRP.
- Kebijakan dan Prosedur anti petir dan *grounded*.
- Prosedur koreksi kesalahan entry.
- Kebijakan integrasi sistem aplikasi.
- Kebijakan mengukur kinerja dan beban sistem.
- Kebijakan *firewall* pada jaringan lokal.
- Prosedur pemeliharaan perangkat pendukung.
- Kebijakan dan prosedur pencegahan penyebaran virus.
- Prosedur *backup* data dan sistem.

Sasaran yang kedua ialah dapat mengidentifikasi kebutuhan Sumber Daya Manusia (SDM). Sasaran yang ketiga ialah dapat mengidentifikasi pembangunan dan pemeliharaan sistem dari aspek keamanan informasi. Sasaran yang keempat ialah dapat mengidentifikasi aset-aset perusahaan yang kritikal milik perusahaan, serta mengidentifikasi risiko, ancaman dan kerawanannya. Sasaran yang kelima ialah dapat mengidentifikasi insiden keamanan informasi yang berpotensi terjadi.

Sasaran yang keenam ialah dapat mengidentifikasi pengelolaan fisik dan lingkungan keamanan informasi. Sasaran yang ketujuh ialah dapat mengidentifikasi pengelolaan komunikasi dan operasional keamanan informasi. Sasaran yang kedelapan ialah dapat melakukan audit dan selanjutnya korektif terhadap kesalahan atau gangguan yang terjadi.

Sasaran yang kesembilan ialah dapat mengidentifikasi pengelolaan keberlanjutan bisnis, yang perlu dilakukan.

Tabel 4. Rencana Keamanan Informasi

No	Strategy	No	Security Control
1	Menyusun kebijakan, prosedur dan standard terkait dengan keamanan informasi	1	Kebijakan dan prosedur
		2	Labelling of sensitive material
		3	Penyimpanan backup data pada tempat aman
2	Menyempurnakan pola rekruitmen dan pelatihan dan pengelolaan SDM TI	4	Pemeriksaan latar belakang
		5	Perjanjian kerja
		6	Pelatihan security awareness
		7	Sharing responsibilities
		8	Job rotation
		9	Increased supervisions
3	Mengimplementasikan perangkat preventive and detection serangan dan gangguan	10	Scanning terhadap virus
		11	Pemasangan anti petir dan ground
		12	Pemasangan firewall
		13	Intrussion Detection System
		14	Enkripsi
		15	Pembatasan fungsi dan informasi
		16	Penggunaan call back system
4	Menerapkan pola pemeriksaan dan evaluasi operasional TI terkait keamanan informasi	17	Violation report
		18	Audit trail information

Strategi

Strategi keamanan informasi merupakan bagian penting dari rencana yang komprehensif untuk keamanan informasi dan komunikasi. Pada setiap strategi tersebut, akan disampaikan kumpulan aksi yang perlu dilakukan dalam pelaksanaan strategi tersebut, dalam upaya mencapai tujuan dan sasaran yang telah ditentukan.

Strategi yang pertama ialah menyusun kebijakan, prosedur dan standard terkait dengan keamanan informasi. Strategi ini dijalankan dengan melakukan identifikasi terhadap kebijakan, prosedur dan standard yang penting untuk disusun dan ditetapkan

Strategi yang kedua ialah menyempurnakan pola rekuitmen dan pelatihan SDM TI. Strategi ini dijalankan dengan melakukan pemeriksaan latar belakang dari calon karyawan TI.

Strategi yang ketiga ialah mengimplementasikan perangkat preventive dan detection terhadap serangan dan gangguan keamanan informasi. Strategi ini dijalankan dengan melakukan scanning virus secara teratur, serta memperbaharui perangkat anti virus secara berkala.

Strategi yang keempat ialah menerapkan pola pemeriksaan dan evaluasi operasional TI terkait keamanan informasi. Strategi ini dijalankan dengan melakukan peningkatan kegiatan pengawasan terhadap kerja dari para operator yang berjumlah cukup banyak, agar terkelola autentifikasi dan otoritas yang telah diberikan.

Kontrol Keamanan

Tujuan rencana keamanan dapat dicapai jika sasaran yang telah ditentukan telah dipenuhi. Selanjutnya setiap sasaran hanya dapat dicapai jika menerapkan beberapa strategi keamanan informasi, dan setiap strategi memberikan rekomendasi aksi yang harus dilakukan, sebagai upaya mencapai sasaran yang telah ditentukan.

Adapun kontrol keamanan tersebut, dapat dilihat pada Tabel 4. Strategi dan kontrol keamanan diperoleh berdasarkan hasil proses penilaian dan mitigasi risiko. Penilaian risiko menghasilkan tingkatan risiko dan rekomendasi kontrol keamanannya, berdasarkan penilaian yang dilakukan terhadap delapan aspek, yaitu:

1. Pengelolaan kebijakan keamanan informasi
2. Pengelolaan aset perusahaan
3. Pengelolaan SDM keamanan informasi
4. Pengelolaan fisik dan lingkungan keamanan informasi
5. Pengelolaan komunikasi dan operasional
6. Pengelolaan pembangunan sistem dan pemeliharaannya
7. Pengelolaan insiden keamanan informasi
8. Pengelolaan keberlanjutan bisnis

Kumpulan risiko dan tingkatannya selanjutnya dijadikan dasar dalam merekomendasikan kontrol keamanan yang dapat mencegah atau menurunkan risiko tersebut, sehingga proses penilaian risiko akan menghasilkan beberapa hal, yaitu:

a. Risiko yang diperoleh dari kelemahan/kerawanan dan ancamaan terhadap aset kritikal yang dimiliki perusahaan
b. Nilai risiko yang diperoleh dari kecenderungan dan dampak yang dapat ditimbulkan oleh risiko tersebut jika terjadi.
c. Rekomendasi kontrol keamanan informasi, berdasarkan risiko yang dimitigasi.

Tahapan *risk* mitigasi, telah menghasilkan beberapa hal, yaitu:

a. Prioritas aksi yang harus dilakukan dalam rangka memitigasi risiko.
b. Hasil evaluasi terhadap kontrol keamanan yang direkomendasikan. Hasil evaluasi tersebut berupa kesesuaian kontrol terhadap kelemahan/kerawanan yang dihilangkan atau dikurangi, serta efektivitas kontrol dalam menurunkan risiko yang dapat timbul akibat kerawanan/kelemahan tersebut.
c. Hasil analisis *cost-benefit* terhadap kontrol keamanan yang direkomendasikan. Hasil analisis ini menjelaskan manfaat dan kerugian, jika kontrol ini diimplementasikan atau tidak diimplementasikan, sehingga menjadi pertimbangan bagi perencanaan keamanan informasi.
d. Hasil analisis *cost-effectiveness* terhadap kontrol keamanan yang direkomendasikan. Hasil analisis ini menjelaskan perbandingan efektivitas antar kontrol terhadap pencapaian tujuan keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*, sehingga memberikan usulan prioritas implementasi dari seluruh kontrol yang direkomendasikan.
e. Rencana kontrol keamanan, yang berisi tentang keburuhan sumber daya yang harus disiapkan untuk mengimplementasikan kontrol-kontrol keamanan tersebut, serta tim yang dibentuk untuk mengimplementasikannya.

Rencana keamanan yang komprehensif telah disusun, berdasarkan tahapan penilaian risiko (*risk assessment*) dan *risk* mitigasi, sehingga secara lengkap memberikan pertimbangan dan dasar dalam menentukan tujuan, sasaran, strategi dan kontrol keamanan untuk menjamin keamanan informasi di perusahaan.

Kontrol keamanan yang dipilih dan digunakan untuk mencapai sasaran keamanan informasi. Terdapat tiga jenis kontrol yang digunakan, yaitu kontrol management (*management control*), kontrol operasional (*operational control*), dan kontrol teknikal (*technical control*).

Kontrol kebijakan dan kontrol internal perusahaan yang ada dalam rencana keamanan ini, harus dikelola secara baik. William Conner (2004) menjelaskan bahwa tata kelola keamanan informasi merupakan salah satu bagian dari konsep tata kelola organisasi yang baik (*good organization governance*), yang terdiri atas sekumpulan kebijakan dan kontrol internal perusahaan yang terkoordinasi dan terkelola [7].

KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian ini, ialah:

1. Analisis risiko menghasilkan tingkatan risiko, berdasarkan identifikasi kelemahan, ancaman dan kecenderungan, yang dihadapi oleh perusahaan, serta rekomendasi kontrol keamanan untuk menurunkan risiko. Berdasarkan hasil penilaian risiko, perusahaan ini memiliki risiko tinggi (*high*) sehingga akan kehilangan informasi. Risiko tersebut harus diturunkan dengan mengimplementasikan beberapa kontrol keamanan yang direkomendasikan.
2. Pada tahap mitigasi risiko, perusahaan dapat melakukan evaluasi dan analisis terhadap kontrol keamanan yang direkomendasikan. Evaluasi tersebut meliputi kesesuaian dan efektifitas, sedangkan analisis yang dilakukan menggunakan teknik analisis *cost-effectiveness* dan *cost-benefit*. Berdasarkan hasil mitigasi risiko, maka perusahaan memperoleh prioritas implementasi kontrol-kontrol keamanan, dalam upaya menurunkan risiko yang terdiri atas delapan belas kontrol keamanan.
3. Rencana keamanan informasi disusun berdasarkan tujuan dan sasaran keamanan informasi perusahaan, yang didukung oleh hasil penilaian dan mitigasi risiko yang komprehensif. Sehingga dapat menjadi panduan dalam penerapan keamanan informasi, dengan langkah implementasi kontrol keamanan, untuk mencapai tujuan dan sasaran keamanan informasi.

DAFTAR PUSTAKA

1. Sodiq, A., 2009, *Aspek Keamanan Informasi* 2009.
2. Rawson, B. S., 2007, *State Enterprise Security Plan*.
3. *Information Ass Spring, Security Planning and Risk Analysis*, CS461, 2008.
4. Mell, P., 2002, *Use of Common Vulnerabilities and Exposure (CVE) Vulnerability Naming Scheme*.
5. Krutz, R. L. dan Vines, R. D., 2003, *The CISSP Preparation Guide*, Wiley Publishing.
6. Peltier, T. R., 2001, *Information Security Risk Anaysis*, Auerbach Publications.
7. Conner, F. W., 2004, *Information Security Governance (ISG)*.