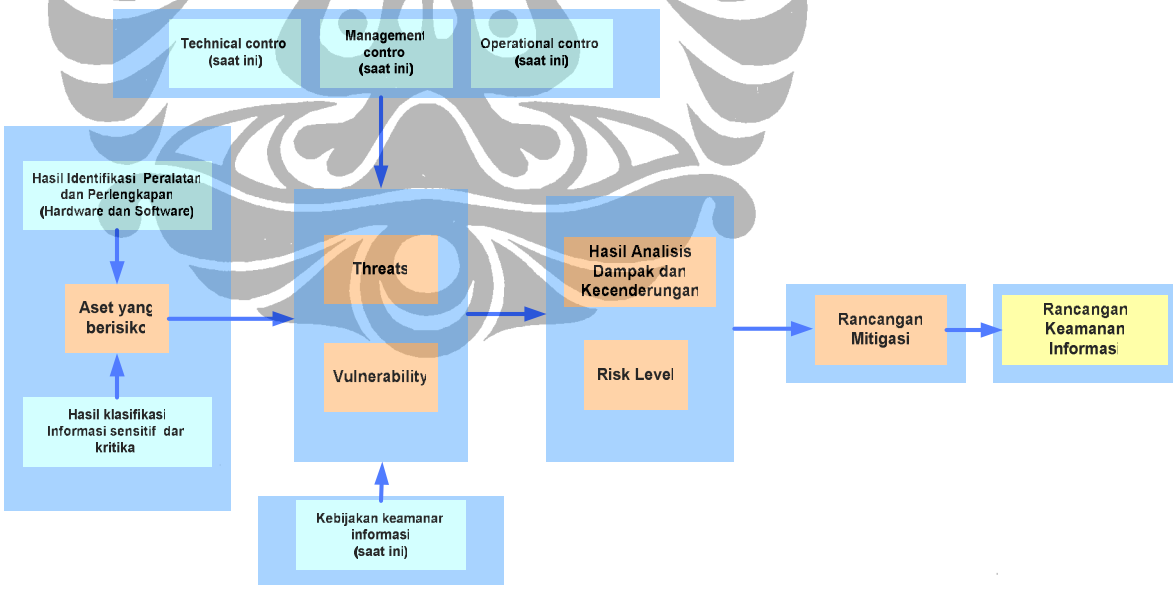
BAB 3 DESAIN DAN METODOLOGI PENELITIAN

3.1 Desain Penelitian

Desain penelitian bertujuan untuk menggambarkan pola pikir yang menuntun arah penelitian, untuk menghasilkan keluaran yang menjadi produk atau hasil penelitian. Terdapat bangunan dari penelitian ini, meliputi informasi tentang aset yang berisiko, yang teridentifikasi memiliki ancaman dan kerawanannya. Penelitian ini juga membutuhkan informasi tentang kontrol-kontrol yang telah dimiliki oleh perusahaan, yang terdiri dari kontrol teknikal, manajemen dan operasional serta kebijakan dan prosedur, yang akan memperngaruhi dalam analisis dampak dan tingkat risiko. Hasil analisis dampak dan tingkat risiko, selanjutnya akan menjadi dasar dalam sebuah rancangan mitigasi risiko dan rancangan keamanan informasi.



Gambar 3.1 Desain Penelitian

Adapun penjelasan dari desain bangunan penelitian ini, sebagai berikut:

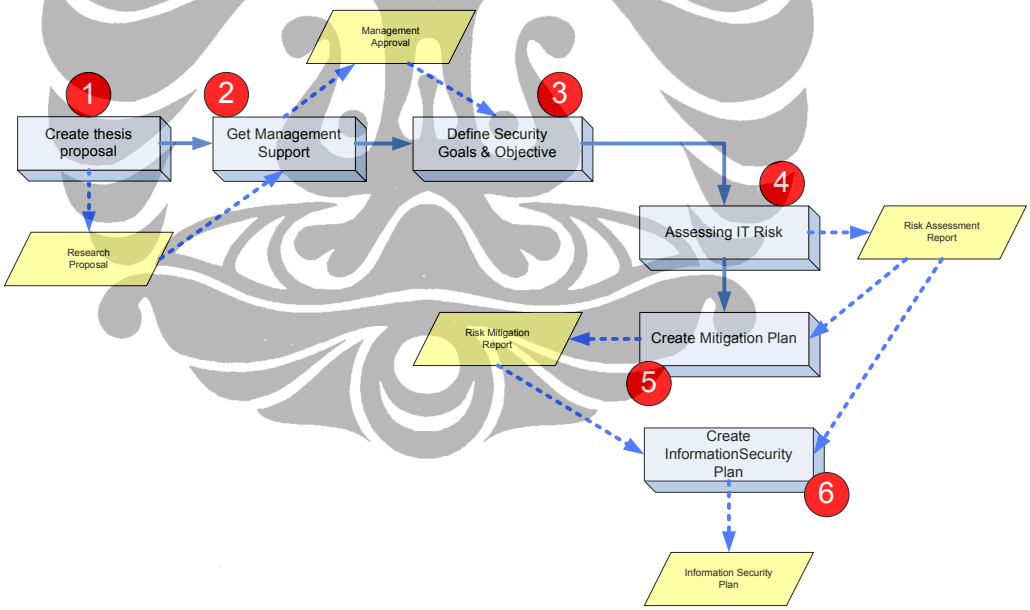
- Informasi aset yang beresiko, diperoleh dari hasil identifikasi mengenai spesifikasi aplikasi pendukung proses bisnis, perangkat lunak dan keras yang digunakan oleh perusahaan, juga informasi mengenai aliran informasi yang terjadi antar pihak/entitas di perusahaan, dan dari hasil klasifikasi informasi sensitif dan kritikal bagi perusahaan. Dengan informasi ini, maka akan dapat ditentukan aset-yang beresiko, yang dimiliki perusahaan, sehingga harus dilindungi.
- Ancaman dan kerawanan/kelemahan melekat pada aset-aset penting milik perusahaan, yang berpengaruh pada potensi hilangnya keamanan informasi, yang dapat mengganggu jalannya bisnis perusahaan. Ancaman dan kerawanan/kelemahan diperoleh dari hasil identifikasi dan analisis kebijakan dan kontrol keamanan yang saat ini dimiliki oleh perusahaan.
- Analisis dampak dan kecenderungan berdasarkan ancaman dan kerawanan/kelemahan yang teridentifikasi, selanjutnya akan menghasilkan tingkat risiko.
- Rancangan mitigasi risiko, menjadi strategi untuk menjelaskan bahwa tingkat risiko dan analisis dampak, akan dijadikan dasar dalam merencankan langkah-langkah untuk meredam atau mengurangi resiko.
- Rancangan keamanan informasi, dapat memberikan panduan dalam melakukan implementasi kontrol keamanan informasi bagi perusahaan, berdasarkan rekomendasi rancangan mitigasi risiko, dan penilaian tingkat risiko, sehingga secara efektif mendukung tercapainya keamanan informasi.

Desain penelitian yang menjadi kerangka berfikir dalam melakukan penelitian, akan dijalankan dalam rangkaian sistematis langkah-langkah penelitian, dalam sebuah metodologi penelitian, sehingga dalam setiap tahapan dalam metodologi penelitian tersebut, dapat dipilih metode dan teknik untuk menghasilkan keluaran yang sesuai dengan hasil akhir penelitian pada desain penelitian. Penjelasan tentang metodologi penelitian, akan dibahas pada bagian selanjutnya.

3.2 Metodologi Penelitian

Metodologi penelitian merupakan rangkaian tahapan sistematis yang dilakukan untuk menyelesaikan dan menjawab pertanyaan penelitian ini yang telah ditentukan. Rangkaian tahapan pada metodologi penelitian ini terdiri dari enam tahapn, meliputi:

1. Membuat proposal tesis *(create thesis proposal)*
2. Meminta dukungan dari perusahaan *(get management support)*
3. Mendefinisikan tujuan and sasaran keamanan informasi yang ingin dicapai *(define security goals and abjectives)*
4. Menilai risiko teknologi informasi perusahaan *(asssess IT risk)*
5. Membuat rancangan mitigasi risiko *(create mitigation plan)*
6. Membuat rancangan keamanan informasi *(create information security plan)*



Gambar 3.2 Metodologi Penelitian

Penjelasan tahapan diatas, sebagai berikut:

- *Create Thesis Proposal,* merupakan langkah pertama pada penelitian ini, yaitu membuat proposal penelitian/tesis. Keluaran dari tahapan ini adalah proposal penelitian/tesis.
- *Get Management Support*, yaitu melakukan pengajuan izin ke perusahaan tempat penelitian, agar diperoleh dukungan dari pimpinan perusahaan untuk melakukan penelitian. Pengajuan izin dilakukan dengan membawa surat keterangan dari sekretariat Magister Teknologi Informasi UI, dan melampiran proposal penelitan yang telah disusun, untuk diserahkan kepada pimpinan perusahaan, tempat penelitian dilakukan. Keluaran dari tahapan ini adalah surat persetujuan pimpinan perusahaan untuk menjadi objek penelitan dari tesis ini.
- *Define Security Goals and Objective,* yaitu melakukan wawancara awal dengan pimpinan divisi yang terkait, untuk menentukan sasaran keamanan informasi.
- *Assessing IT Risk*, yaitu melakukan penaksiran/penilaian risiko teknologi informasi, dengan tahapan pada risk assessment. Teknik yang digunakan pada tahapan ini adalah observasi dan wawancara, dan IT Risk Analysis. Keluaran dari tahapan ini adalah Laporan Penaksiran/Penilaian Risiko TI.
- *Create Mitigation Plan*, yaitu melakukan perancangan untuk meminimalisasi dan mengurangi risiko, berdasakan hasil dari penaksiran/penilaian risiko TI. Teknik yang dilakukan pada tahapan ini adalah cost-benefit analysis.
- *Create Information Security Plan*, yaitu melakukan perancangan keamanan informasi untuk perusahaan, berdasarkan hasil penaksiran/penilaian risiko.

Berdasarkan penjelasan metodologi diatas, maka terlihat dengan jelas, tentang langkah-langkah dalam melakukan penelitian, untuk menjawab pertanyaan penelitian. Penjelasan lebih rinci mengenai tahapan *Assessing IT Risk, Create Mitigation Plan*, dan *Create Information Security Plan* akan dijelaskan pada bagian selanjutnya.

3.3 Tahapan Penilaian Risiko TI

Gary Stonebumer (2006) menjelaskan bahwa penilaian risiko merupakan langkah-langkah yang dilakukan dalam rangka untuk mengetahui tingkat risiko terhadap aset miliki perusahaan, dan rekomendasi kontrol keamanannya, karena dari hasil tahapan ini akan menentukan rancangan untuk mengurangi resiko terhadap keamanan informasi.

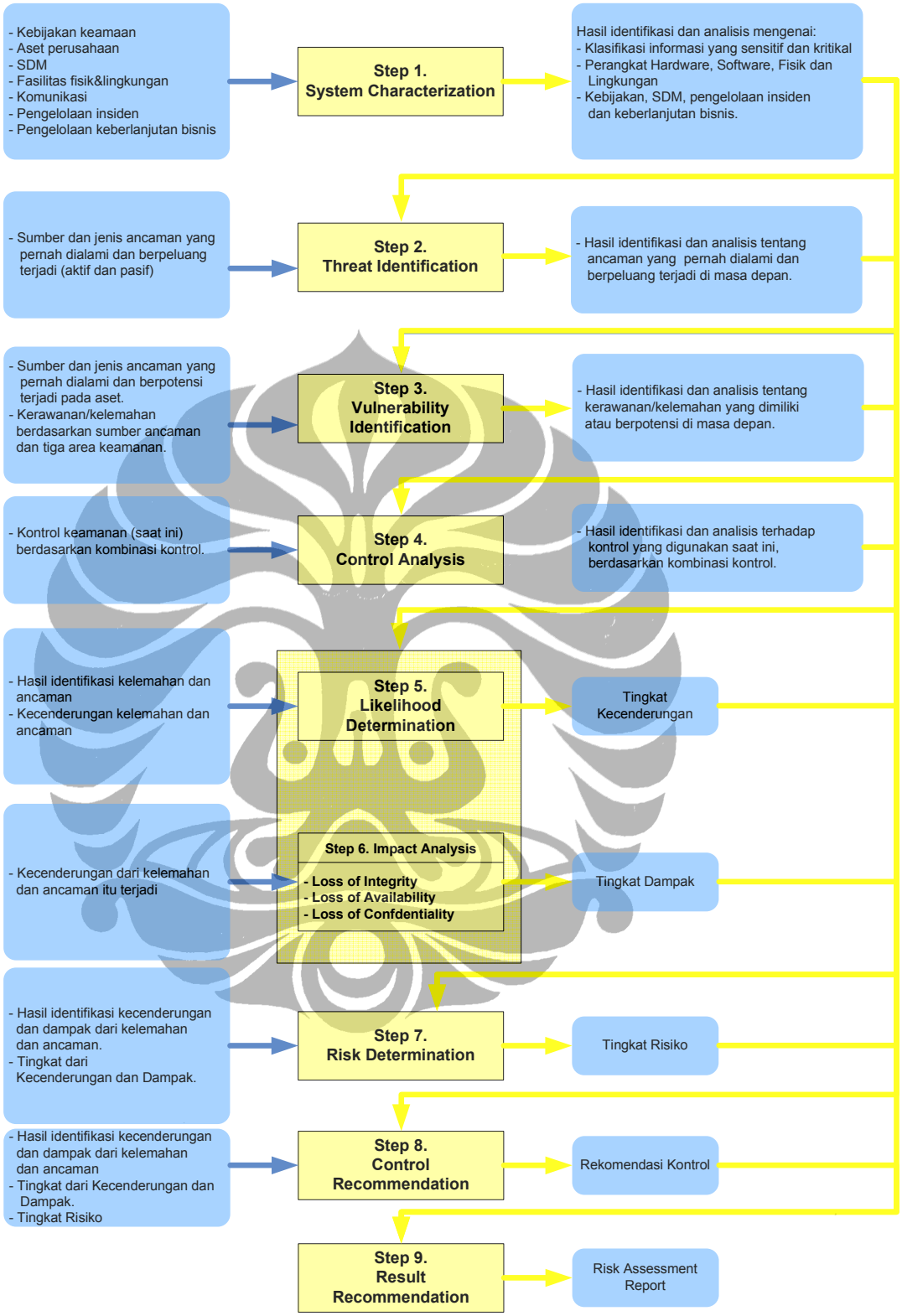
Adapun langkah-langkah dalam penilaian risiko TI, sebagai berikut:

1. Identifikasi karakteristik sistem (*system characterization)*
2. Identifikasi ancaman (*threat identification)*
3. Identifikasi kerawanan/kelemahan (*vulnerability determination)*
4. Analisis kontrol (*control analysis)*
5. Pengenalan kecenderungan (*likelihood determination)*
6. Analsis dampak (*impact analysis)*
7. Pengenalan risiko (*risk determination)*
8. Rekomenfasi kontrol (*control recommendation)*
9. Dokumentasi (*result documentation)*

Berikut ini penjelasan dari langkah-langkah pada penilaian risiko:

1. Identifikasi karakteristik sistem (*system characterization)*, merupakan proses identifikasi dan analisis kebijakan keamanan saat ini, aset perusahaan, pengelolaan sumber daya manusia terkait dengan implementasi keamanan informasi, fasilitas fisik dan lingkungan, komunikasi dan sosialisasi kepedulian tentang keamanan informasi, serta pengelolaan insiden dan keberlanjutan bisnis.
2. Identifikasi ancaman (*threat identification)*, merupakan proses identifikasi dan analisis terhadap sumber dan jenis ancaman yang pernah atau berpeluang terjadi, baik ancaman aktif dan pasif.

3. Identifikasi kerawanan/kelemahan (*vulnerability determination)*, merupakan proses identifikasi kerawanan berdasarkan sumber ancaman dan tiga area keamanan, serta analisis kerawanan/kelemahan yang dimiliki atau berpotensi terjadi dimasa depan.
4. Analisis kontrol (c*ontrol analysis),* merupakan proses identifikasi dan analisis terhadap kontrol yang digunakan saat ini berdasarkan kombinasi kontrol.
5. Pengenalan kecenderungan (*likelihood determination)*, merupakan proses identifikasi dan analisis terhadap kecenderungan kelemahan dan ancaman dapat terjadi, sehingga dapat dihasilkan tingkat kecenderungan.
6. Analisis dampak (i*mpact analysis),* merupakan proses identifikasi dan analisis terhadap dampak dari kerawanan/kelemahan dan ancaman yang dapat terjadi, sehingga dihasilkan tingkat dampak.



Gambar 3.3 Tahapan *Risk Assessment*

7. Pengenalan risiko (*risk determination)*, merupakan proses identifikasi dan analisis terhadap hasil identifikasi kecenderungan dan dampak berdasarkan kerawanan/kelemahan dan ancaman, serta tingkat kecenderungan dan dampak..
8. Rekomendasi kontrol (c*ontrol recommendation)*, merupakan proses untuk menyampaikan beberapa rekomendasi kontrol yang dapat diharapkan mampu meredakan atau mengurangi risiko yang ada.
9. Dokumentasi (*result documentation)*, merupakan proses menyusun dokumentasi terhadap keseluruhan hasil dari penilaian risiko yang telah dilakukan.

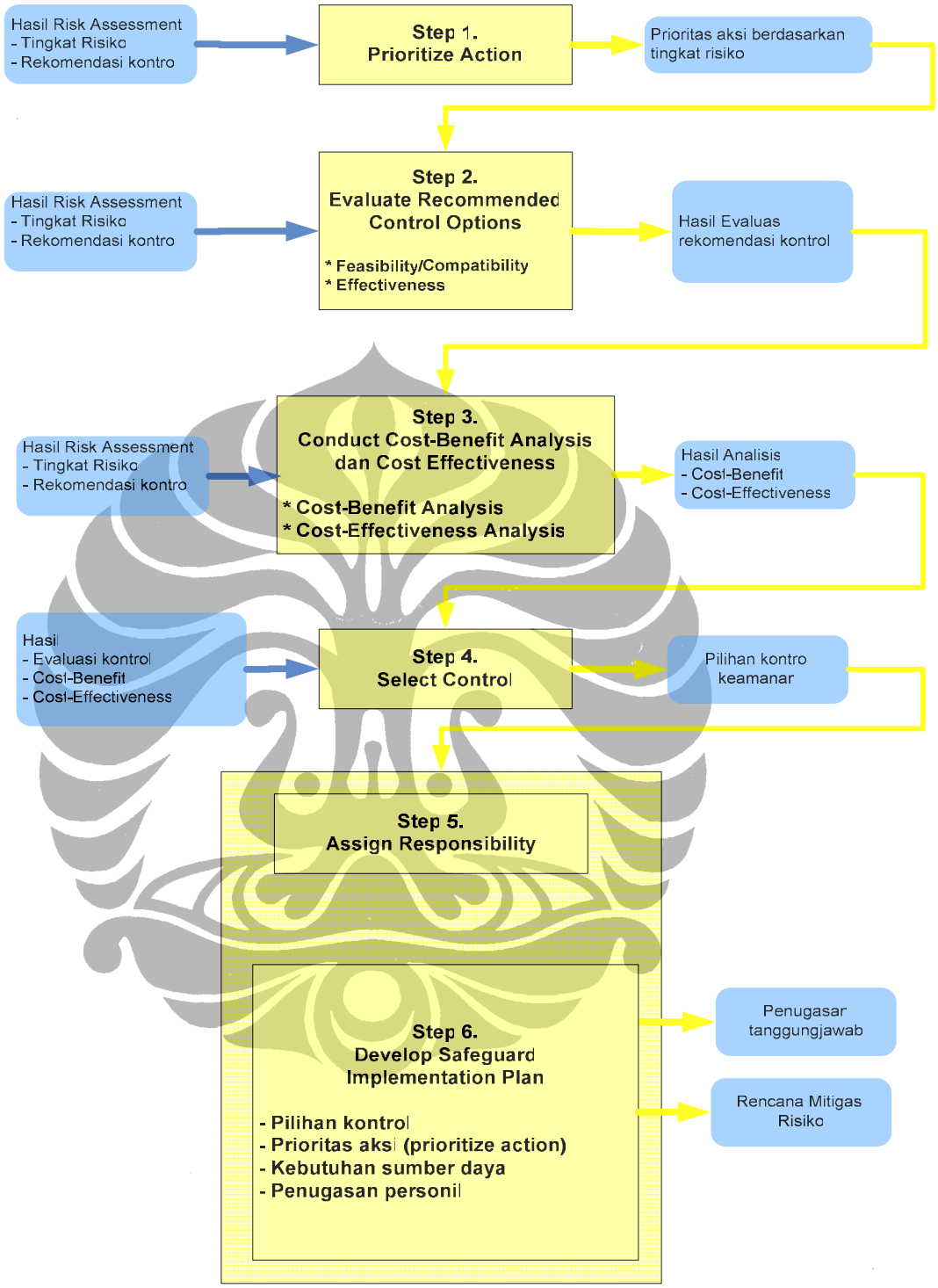
Salah satu hasil dari penilaian risiko ialah tingkat risiko dan rekomendasi kontrol keamanan. Selanjutnya kontrol keamanan tersebut perlu dievaluasi dan dianalisis nilai manfaat dan biaya, serta efektivitas dengan teknik analisis. Analisis tersebut dilakukan pada tahapan *risk mitigation*, yang akan dijelaskan pada bagian selanjutnya.

3.4 Tahapan Mitigasi Risiko

Stonebumer (2006) menjelaskan bahwa rancangan meredam atau mengurangi risiko merupakan langkah-langkah yang harus dilakukan sebagai upaya mengurangi risiko kehilangan atau kerusakan terhadap aset yang dimiliki oleh perusahaan.

Terdapat enam proses utama dalam melakukan *risk mitigation*, yang perlu dilakukan oleh pimpinan perusahaan dalam meminimalisasi risiko, tahapan tersebut meliputi :

1. Prioritas aksi (*prioritize action)*
2. Evaluasi Kontrol yang direkomendasikan (a*valuate rekommended control options)*
3. Melakukan analisis cost-benefit (*conduct cost-benefit analysis)*
4. Pemilihan Kontrol (*select control)*
5. Penugasan Tanggung jawab (*assign responsibility)*
6. Membangun rancangan implementasi keamanan (*develop a safeguard implementation plan)*



Gambar 3.4 Tahapan *Risk Mitigation*

Berikut ini adalah penjelasan dari setiap langkah risk mitigation :

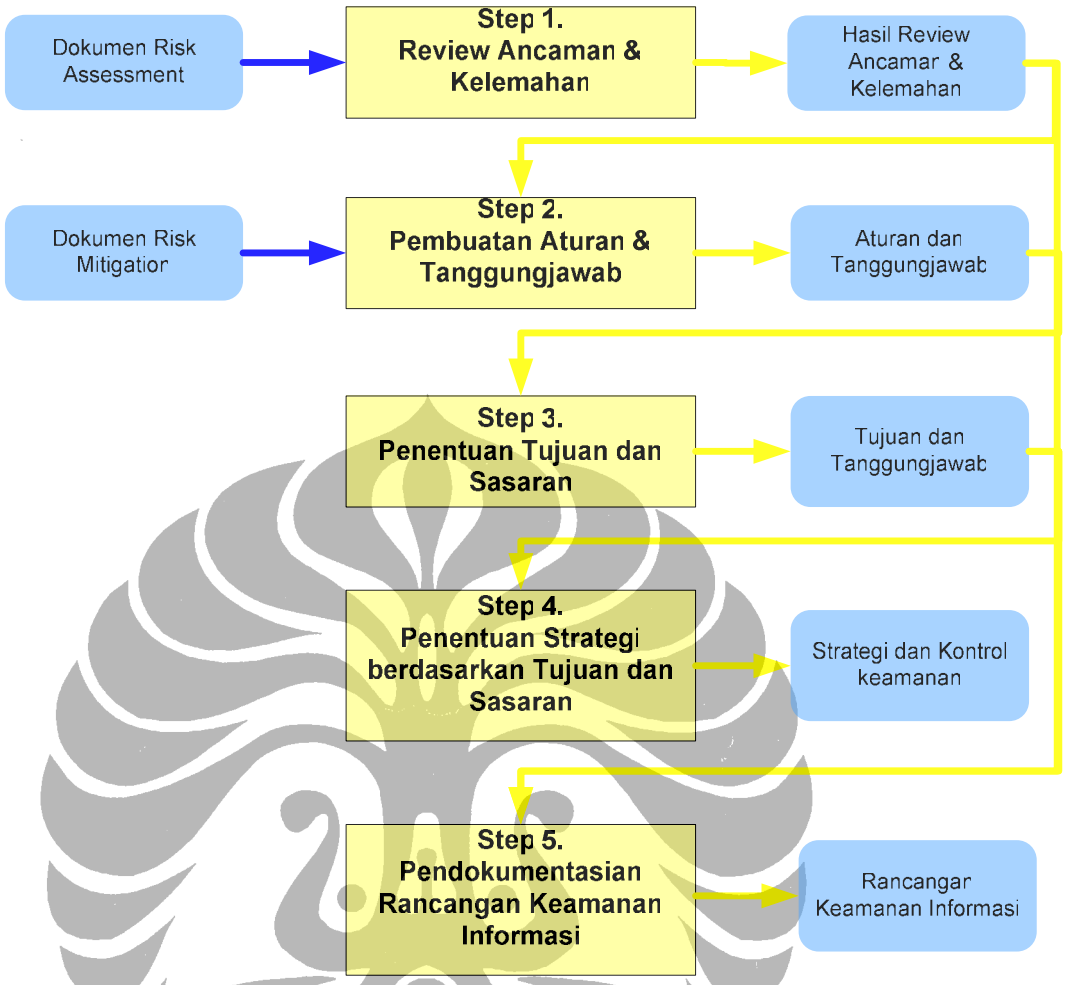
1. *Prioritize Action*, merupakan proses untuk melakukan penentuan prioritas, berdasarkan tingkat penilaian risiko. Dalam pengalokasian sumber daya yang diperlukan, dibutuhkan prioritas yang akan menginformasikan tentang tingkat risiko berdasarkan rankingnya. Adapun output dari proses ini adalah ranking dari tindakan (*actions*) yang perlu dilakukan dari ranking tinggi ke rendah.
2. *Evaluate Recommended Control Options,* merupakan proses untuk melakukan evaluasi untuk dapat menilai tingkat fisibility dan efektivitas dalam penetapan strategi pengamanan, berdasarkan prioritas aksi yang telah ditentukan pada proses sebelumnya. Adapun hasil dari proses ini adalah informasi mengenai *feasible* control.
3. *Conduct Cost-Benefit Analysis dan Cost-effectiveness analysis*, merupakan proses analisis cost-benefit, yang akan menilai nilai manfaat dibandingkan biaya, jika mengimplementasikan kontrol atau tidak. Serta analisis cost effectiveness, untuk mengetahui efektivitas dari usulan kontrol, sehingga dapat diketahui prioritas dari kontrol.
4. *Select Control*, merupakan proses pemilihan kontrol, berdasarkan hasil analisis cost-benefit dan cost effectiveness serta tingkat risiko hasil penilaian risiko.
5. *Assign Responsibility*, merupakan proses untuk menugaskan kepada seseorang yang tentunya memiliki potensi dan kemampuan, dalam mengimplementasikan strategi komtrol yang telah ditentukan diatas. Adapun hasil dari proses ini adalah list dari beberapa orang yang diserahi tanggungjawab.
6. *Develop a Safeguard Implementation Plan*: merupakan proses untuk menentukan rancangan implementasi kontrol keamanan yang telah dipilih. Adapun hasil dari proses ini adalah *safeguard implementation plan.*
7. *Implement Selected Control,* merupakan proses untuk mengimplementasikan kontrol, dimana terdapat kemungkinan tidak dapat menghilangkan risiko tersebut.

Hasil dari tahapan risk mitigation, ialah piluhan kontrol yang telah dianalisis nilai manfaat dan efektifitasnya. Sebelum kontrol tersebut diimplementasikan, perlu dibuat sebuah rancangan keamanan informasi, yang dapat menjelaskan strategi keamanan informasi berdasarkan hasil penilaian risiko dan mitigasi risiko. Pembahasan tentang tahapan perancangan keamanan informasi, akan dijelaskan pada tahapan selanjutnya.

3.5 Tahapan Perancangan Keamanan Informasi

Menurut Rawson (2007) pada dokumen yang berjudul "State Enterprise Security Plan, " pembuatan rancangan keamanan informasi pada organisasi tertentu dilakukan dengan tahapan sebagai berikut:

1. Review ancaman dan kerawanan/kelemahan (*Threats and Vulnerabilities*).
2. Pembuatan aturan dan tanggung jawab (*Roles and Responsibilities*).
3. Penentuan tujuan dan sasaran (*Goals and Objective*).
4. Penetapan Startegi berdasarkan tujuan dan sasaran. (*Strategy*)
5. Pendokumentasian rancangan keamanan informasi.



Gambar 3.5 Tahapan Rancangan Keamanan Informasi

Berikut ini penjelasan mengenai langkah-langkah pada pembuatan rancangan keamanan informasi:

1. Review ancaman dan kelemahan, merupakan proses untuk mereview hasil tahapan penilaian risiko, dengan mengambil informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi jika terjadi (ancaman), yang memanfaatkan kerawanan/kelemahan yang dimiliki oleh perusahaan.
2. Pembuatan aturan dan tanggungjawab, merupakan proses menyusun aturan dan penanggungjawab, yang akan mengatur kegiatan sebagai upaya untuk menurunkan risiko yang bersumber dari ancaman dan kelemahan

3. Penentuan 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.
4. Penentuan strategi, 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.
5. Pendokumentasian rancangan keamanan informasi, merupakan proses untuk menyusun dokumen rancangan keamanan berdasarkan hasil-hasil yang telah dilakukan pada tahap perancangan keamanan informasi.

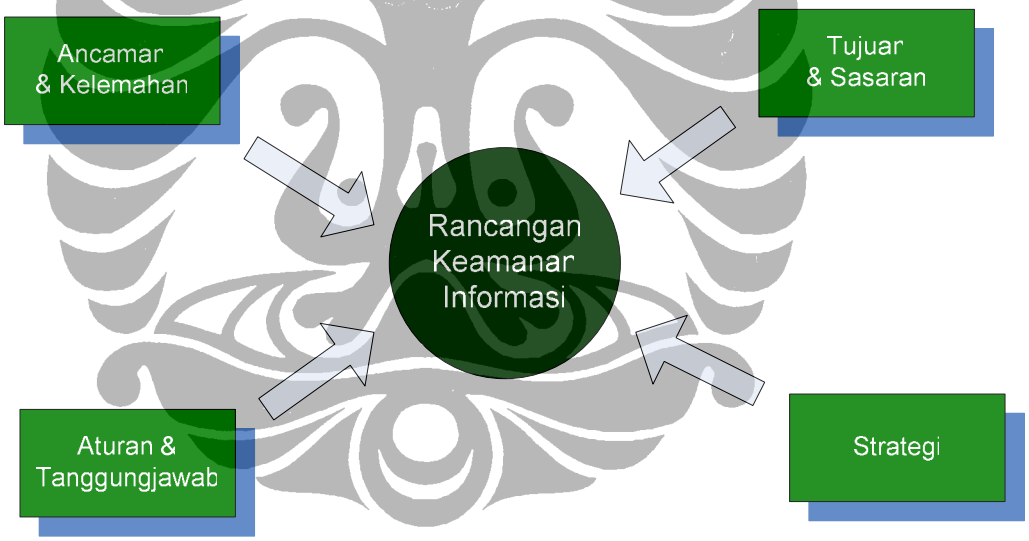
Hasil akhir penelitian ini adalah sebuah rancangan keamanan yang disusun berdasarkan penilaian risiko serta mitigasi risiko, sehingga pilihan strategi dan kontrol yang akan diimplementasikan dapat secara efektif memberikan keamanan informasi, dengan cara menurunkan risiko gangguan keamanan informasi yang mungkin dihadapai oleh organisasi atau perusahaan. Setelah tahapan penelitian secara detail dijelaskan serta hasil-hasil yang akan diperoleh dari penelitian ini, maka akan dilakukan penilaian risiko, mitigasi dan perancangan keamanan dengan studi kasus pada PT.Multi Terminal Indonesia, yang akan dibahas pada bagian selanjutnya.

BAB 6 PERANCANGAN KEAMANAN INFORMASI PERUSAHAAN

6.1 Pendahuluan Rancangan Keamanan

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

Rancangan keamanan informasi terdiri dari empat hal penting yaitu informasi ancaman dan kelemahan, aturan dan tanggung jawab, tujuan dan sasaran, dan strategi.



Gambar 6.1Kerangka Rancangan Keamanan Informasi

Ancaman dan kelemahan akan 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 dilakukan 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 sebagai upaya untuk menurunkan risiko dari terjadinya gangguang 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 di capai sesuai dengan tujuan keamanan yang ditetapkan.

Strategi akan 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.

6.2 Ancaman dan Kelemahan

Ancaman dan kerawanan/kelemahan dapat menggambarkan risiko yang berpotensi diterima oleh perusahaan, berdasarkan aset-aset TI yang dinilai pada tahap penilaia risiko (*risk assessment*), maka dapat dihasilkan informasi kerawanana/kelemahan dan ancamaan, sebagai berikut:

Tabel 6.1 Ancaman dan Kelemahan (1)

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 memilk alternatif cara agar bisnis dapat terus berjalan, sehingga yang terjadi bisnis terhenti dan perusahaan mengalami kerugian.			√	H
3	Petir di lokasi tersebut, intensitasnya cukup besar, dan peralatan penangkal (antipetir 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 serve 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 file data.	Sistem operasi yang rentan dengan penyebaran virus, dapat berpotensi merusak informasi dan mengganggu jaringan komputer perusahaa.			√	H
6	Penggunaan firewall hanya pada sisi luar DMZ saja, berpotensi terbukanya wilayah server dari gangguan yang berasal dari dalam jaringan (lokal), karena area dalam DMZ tidak dilindungi firewall	Penyusupan dan gangguan yang berasal dari jaringan lokal dapat langsung masuk ke area DMZ dimana server berada, dan mengakses informasi dan sistem yang sensitif dan kritikal.	√	√	√	H

Tabel 6.2 Ancaman dan Kelemahan (2)

No	Vulnerability	Threat	C	I	A	Risk
7	Tidak dilakukan pengujian terhadap file hasil backup sistem dan data.	Jika terjadi kehilangan data pada sistem utama, maka hasil backup tidak dapat direstore, terjadi kehilangan informasi.			√	H
8	Pegawai yang telah menguasai bisnis proses dan pengelolaan teknologinya, masih berstatus pegawai kontrak,	Berpotensi pegawai IT dapat keluar kapan pun dari perusahaan dan divisi IT kekurangan pegawai terlatih.	√	√	√	M
9	Karyawan di divisi TI yang cenderung bergant-ganti, sehingga dengan teknologi yang dgunakan oleh perusahaan, membutuhkan keterampilan dan pengetahuan yang cukup, agar dapat melakukan monitoring dan pemeliharaan terhadap sistem yang ada.	Karyawan pengganti atau baru tidak mampu menguasai teknologi perusahaan secara cepat, sehingga proses monitoring dan pemeliharaaan sistem menjadi lambat dan terhambat.			√	M
10	Terjadi kesalahan input data pada aplikasi di lapangan, dan tidak terdapat prosedur tetap dalam pelaporan dan verifikasi kesalahan tersebut.	Kesalahan input data tersebut jika tidak diverifikasi dan dikoreksi secara cepat, menyebabkan waktu layanan menjadi lama, dan akan menurunkan kepercayaan konsumen terhadap perusahaan.		√		M
11	Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi,	Perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, menyebabkan kelemahan tersebut diketahui orang, yang akan mengganggu keamanan informasi.	√	√	√	M
12	Jika perusahaan memiliki karyawan baru tidak akan pernah mengetahui tentang kebijakan tentang keamanan informasi, karena aturan yang tidak tertulis dan tidak disosialisasikan dengan baik.	Kecerobohan dan kesalahan yang dilakukan karyawan, sehingga menyebabkan gangguan keamanan informasi.	√	√	√	M
13	Aplikasi yang dibangun dengan platform DBMS yang berbeda dan tidak memenuhi standard keamanan informasi pada aplikasi.	Integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi antar data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai.		√	√	M
14	Modifikasi informasi dan pencurian informasi melalui komputer yang tidak mengaktifkan keamanan dekstop, saat pemiliknya tidak berada ditempat.	Terjadinya pengamblan, modifikasi dan kehilangan informasi file yang sensitif dan kritikal pada PC tersebut.	√	√	√	M

Tabel 6.3 Ancaman dan Kelemahan (3)

No	Vulnerability	Threat	C	I	A	Risk

15	Tidak dilakukan pemeliharaan terhadap perangkat pendukung yang kritikal secara rutin dan berkala, seperti pendingin ruangan pada ruang server dan listrik dengan gensetnya.	Pemeliharaan yang tidak dilakukan secara rutin dan berkala terhadap perangkat pendukung, seperti pendingin ruangan, dapat menyebabkan kerusakan secara mendadak, sehingga akan mengganggu terutama ruang yang kritikal seperti data center dan ruang server.			√	M
16	Informasi yang sensitif (rahasia) dapat dilakses dan dicuri oleh orang yang tidak berhak, karena informasi dilindungi oleh teknologi enkripsi pada informasi tersebut.	Informasi sensitif yang dibaca oleh orang yang tidak berhak, akan menyebabkan menurunnya kepercayaan konsumen terhadap perusahaan.	√	√		M
17	Tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.	Tidak diaktifkannya PC firewall, dapat memudahkan masuknya akses yang tidak terotorisasi, sehingga dapat menyebabkan hilangnya informasi, atau modifikasi dan kerusahakan sistem dan informasi.	√	√	√	M
18	Penggunaan aplikasi dan transaksi informasi yang terus bertambah, tidak terukur secara 19baik, sehingga sulit mengetahui kinerja dan beban sistem saat ini.	Kinerja sistem aplikasi dan transaksi data dapat menurun dan mati tiba-tiba, karena tidak pernah terukur secara baik penambahan beban dari waktu ke waktu.			√	M
19	Operator yang berstatus kontrak, berjumlah cukup banyak, dengan penugasan harian, cenderung rentan dengan penyalahgunaan.	Setiap operator diberikan otentikasi dan otorisasi dalam menggunakan aplikasi dan infirmasi, jika tidak diawasi secara baik, dapat berpotensi menjadi insiders yang mengganggu keamanan informasi.	√	√	√	L

Berdasarkan ancaman dan kelemahan diatas, maka perlu selanjutnya menentukan tujuan dan sasaran rancangan keamanan informasi, yang akan dicapai, agar dapat menurunkan risiko yang berpotensi dapat terjadi terhadap perusahaan, berdasarkan ancaman dan kerawanan/kelemahan yang telah diidentifikasi. Dalam penanganan risiko keamanan informasi ini, perlu dibentuk tatakelola keamanan informasi yang baik, agar dapat diambil keputusan dan pertimbangan masalah-masalah keamanan informasi terkait dengan ancaman dan kerawanan/kelemahan yang berhasil diidentifikasi.

6.3 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 (*informatioan 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.

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 respond terhadap kejadian/insiden keamanan informasi dengan melakukan investigasi, mitigasi, dan penuntutan.
- Bertanggungjawab melakukan respond 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.

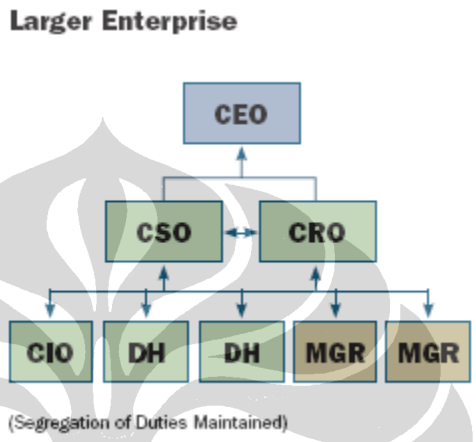
Berdasarkan kumpulan tanggungjawab dan aturan fungsional, maka dapat kelompokkan sebagai berikut:

Gambar 6.2 Tanggungjawab dan aturan fungsional (information securirty governance)

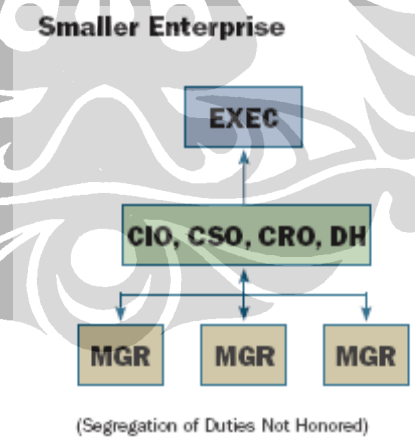
Gambar diatas, menjelaskan hubungan tanggungjawab di bidang keamanan informasi pada sebuah perusahaan, dan aturan fungsional yang terdapat pada strukur organisasi perusahaan, maka pembagian tanggungjawab sebagai berikut:

1. CEO, bertanggungjawab:
   - Bertanggungjawab mengelola secara keseluruhan berjalannya keamanan informasi perusahaan.
   - Bertanggungjawab membuat laporan dan penjelasan kepada konsumen dan umum.
2. CSO/CIO/CRO/DH, bertanggungjawab :
   - Bertanggungjawab merancang kebijakan keamanan, prosedur, program dan pelatiahan keamanan informasi.
   - Bertanggungjawab melakukan respond terhadap kejadian/insiden keamanan informasi dengan melakukan investigasi, mitigasi, dan penuntutan.
   - Bertanggungjawab melakukan respond terhadap laporan hasil audit mengenai keamanan informasi.
   - Bertanggungjawab melakukan audit, penilaian kesesuaian dan kebutuhan terhadap kontrol keamanan.
3. Mid-level Manager, bertanggungjawab:
   - Bertanggungjawab melakukan audit, penilaian kesesuaian dan kebutuhan terhadap kontrol keamanan.
   - Bertanggungjawab mengkomunikasikan dan mensosialisasikan kebijakan, program dan pelatihan kepada seluruh karyawan terkait keamanan informasi.
4. Staf/Karyawan, bertanggungjawab:
   - Bertanggungjawab mengimplementasikan dan melaksanakan seluruh kebijakan, prosedur dan program keamanan informasi, serta melaporkan jika ditemukan kerawanan/kelemahan keamanan.

Tanggungjawab dan aturan fungsional diatas, sangat terkait dengan struktur organisasi yang berlaku di organisasi tersebut, sehingga perlu untuk menampilkan rekomendasi struktur organisasi pada tata kelola keamanan informasi perusahaan, sebagai berikut:



Gambar 6.3 Rekomendasi Struktur Organiasi Keamanan Informasi (Larger)



Gambar 6.4 Rekomendasi Struktur Organisasi Keamanan Informasi (Smaller)

Kedua struktur organisasi yang direkomendasikan oleh konsep tata kelola keamanan informasi, selanjutnya perlu melakukan analisis terhadap struktur organisasi PT. Multi Terminal Indonesia saat ini.

Gambar 6.5 Struktur Organisasi PT. Multi Terminal Indonesia (saat ini)

Struktur organisasi PT. Multi Terminal Indonesia 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.

Aspek SI dan TI merupakan bidang yang strategis menentukan jalannya bisnis perusahaan, sehingga harus ikut mempengaruhi keputusan atau kebijakan tertinggi perusahaan, terutama masalah keamanan informasi perusahaan. Gangguan terhadap keamanan informasi dapat berakibat fatal bagi perusahaan, yaitu hilangnya citra atau nama baik perusahaan dan terhentinya jalannya bisnis perusahaan, sehingga akan memberikan kerugian bagi perusahaan dan mengancam jalannya bisnis perusahaan.

Berdasarkan pertimbangan diatas, maka akan direkomendasikan perubahan secara bertahap struktur organisasi perusahaan, yang mengarah pada tatakelola TI yang baik (IT *good governance*) dan tatakelola keamanan informasi yang baik (*Informatioan Security good governance*) yang semua itu, mengacu pada konsep besar yaitu tatakelola perusahaan yang baik (*corporate good governance*).

6.4 Tujuan dan Sasaran Rancangan Keamanan Informasi

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 rancangan keamanan.

Tabel 6.4 Tujuan dan Sasaran

Goals	Objective
Prevent	1. Dapat menentukan kebijakan yang dibutuhkan dalam mendukung implementasi keamanan informasi.
	2. Dapat mengidentifikasi kebutuhan Sumber Daya Manusia (SDM) dalam mendukung keamanan informasi
	3. Dapat mengidentifikasi pembangunan pemeliharaan sistem dari aspek keamanan informasi
Reduce	4. Dapat mengidentifikasi aset-aset perusahaan yang kritikal milik perusahaan, serta mengidentifikasi risiko, ancaman dan kerawanannya.
	5. Dapat mengidentifikasi insiden keamanan informasi yang berpotensi terjadi.
	6. Dapat mengidentifikasi pengelolaan fisik dan lingkungan keamanan informasi.
	7. Dapat mengidentifikasi pengelolaan komunikasi dan operasional keamanan informasi.
Respond and Recover	8. Dapat melakukan audit dan korektif terhadap kesalahan atau gangguan yang terjadi
	9. Dapat mengidentifikasi pengelolaan keberlanjutan bisnis,

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

6.4.1 Sasaran: Dapat menentuan Kebijakan

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

- Kebijakan dan Prosedur klasifikasi informasi, bermanfaat dalam mengatur pelabelan informasi, yang akan membedakan perlakukan terhadap informasi tersebut.
- Kebijakan dan Prosedur dekstop, bermanfaat untuk mendorong prilaku pengguna komputer di perusahaan, untuk mengaktifkan firewall dan password screen server.
- Kebijakan dan Prosedur pencatatan kejadian gangguan keamanan TI, bermanfaat untuk mengatur tentang kewajiban mencatat dan mendokumentasikan kejadian-kejadian gangguan keamanan TI yang pernah terjadi.
- Kebijakan dan Prosedur Ruang DRC, bermanfaat mengatur penempatan ruang DRC yang berbeda dengan ruangan data center.
- Kebijakan dan Prosedur BCP dan DRP, bermanfaat untuk mengatur tentang rancangan penanggulangan bencana yang akan dilakukan agar bisnis tetap berjalan, meskipun terjadi bencana.
- Kebijakan dan Prosedur anti petir dan grounded, bermanfaat untuk mengatur tentang pemasangan anti petir dan grounded yang handal dan sesuai dengan skala gangguan yang sering terjadi.
- Prosedur koreksi kesalahan entry, bermanfaat untuk mengatur tentang langkah-langkah dalam melakukan koreksi kesalahan.

- Kebijakan integrasi sistem aplikasi, bermanfaat untuk mengatur menggunakan platform aplikasi dan database tertentu, yang harus diperhatikan oleh pengembang atau vendor.
- Kebijakan mengukur kinerja dan beban sistem, bermanfaat untuk mengatur kegiatan prediksi beban sistem dimasa yang akan datang, sehingga dapat mengantisipasi dengan perancangan.
- Kebijakan firewall pada jaringan lokal, bermanfaat bermanfaat untuk mengatur pemasangan firewall pada jaringan lokal, untuk mencegah serangan ke server dari jaringan lokal.
- Prosedur pemeliharaan perangkat pendukung, bermanfaat untuk mengatur waktu dan cara pemeliharaan perangkat pendukung (AC dan Listrik)
- Kebijakan dan prosedur pencegahan penyebaran virus, bermanfaat untuk mengatur kegiatan pencegahan penyebaran virus.
- Prosedur backup data dan sistem, bermanfaat untuk mengatur pengujian hasil backup data dan system.

6.4.2 Sasaran: Dapat mengidentifikasi kebutuhan SDM TI

Sasaran yang kedua ialah dapat mengidentifikasi kebutuhan Sumber Daya Manusia (SDM) dalam mendukung keamanan informasi. Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Dengan mengidentifikasi kebutuhan SDM TI di perusahaan, maka akan dapat menjamin pengelolaan sistem TI yang baik.
- Pekerjaan di bidang TI menuntut perkembangan pengetahun dan keterampilan yang cepat, terutama dibidang keamanan informasi, sehingga dapat meningkatkan efektivitas dan efisiensi dalam mengelola sistem TI dan keamanan TI.

6.4.3 Sasaran: Dapat mengidentifikasi pembangunan sistem

Sasaran yang ketiga ialah dapat mengidentifikasi pembangunan dan pemeliharaan sistem dari aspek keamanan informasi. Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Aplikasi yang saat ini digunakan, dapat terhindar dari serangan dan gangguan keamanan informasi.
- Serta aplikasi yang akan dikembangkan dapat memenuhi standard keamanan informasi.

6.4.4 Sasaran: Dapat mengidentifikasi aset-aset kritikal perusahaan

Sasaran yang keempat ialah dapat mengidentifikasi aset-aset perusahaan yang kritikal milik perusahaan, serta mengidentifikasi risiko, ancaman dan kerawanannya.

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Diketahuinya kelemahan dan ancaman dari gangguan keamanan informasi, berdasarkan kelemahan dan ancaman.
- Dapat menentukan prilaku yang harus diterapkan pada aset-aset kritikal tersebut.

6.4.5 Sasaran: Dapat mengidentifikasi insiden keamanan informasi

Sasaran yang kelima ialah dapat mengidentifikasi insiden keamanan informasi yang berpotensi terjadi.

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Untuk mengetahui insiden serangan atau gangguan yang pernah terjadi, sehingga dapat dianalisis lebih lanjut.
- Hasil analisa terhadap kejadian/insiden tersebut akan menjadi perhatian bagi admin, untuk mengatahui kelemahan dan kerawanan, yang selanjutnya akan ditentukan langkah mitigasi.

6.4.6 Sasaran: Dapat mengidentifikasi pengelolaan fisik dan lingkungan

Sasaran yang keenam ialah dapat mengidentifikasi pengelolaan fisik dan lingkungan keamanan informasi.

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Mengetahui kelemahan dan kerawananan fisik ruangan data center dan DRC, yang ada saat ini.
- Mengetahui ancaman yang berpotensi terjadi dengan posisi atau lokasi gedung, dimana terdapat ruang data center, sehingga dapat melakukan langkah mitigasi terhadap risiko dari ancaman tersebut.

6.4.7 Sasaran: Dapat mengidentifikasi pengelolaan komunikasi

Sasaran yang ketujuh ialah dapat mengidentifikasi pengelolaan komunikasi dan operasional keamanan informasi.

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Mengetahui bagaimana perusahaan mengkomunikasikan mengenai standard dan prosedur keamanan informasi yang diterapkan, sehingga dapat memberikan solusi sosialisasi kebijakan, standard dan prosedur keamaanan.
- Mendorong tersosialisasinya kebijakan, standard dan prosedur keamanan informasi.

6.4.8 Sasaran: Dapat melakukan audit dan korektif

Sasaran yang kedelapan ialah dapat melakukan audit dan selanjutnya korektif terhadap kesalahan atau gangguan yang terjadi.

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Perusahaan dapat mengetahui dan melacak terjadian kesalahan atau gangguan terhadap sistem dan perangkatnya.
- Setelah diketahui sumber kesalahan tersebut, kemudian dapat melakukan recovery menggunakan file backup atau dokumen fisik, sehingga informasi dapat kembali dikembalikan ke kondisi benar.

6.4.9 Sasaran: Dapat mengidentifikasi pengelolaan keberlanjutan bisnis

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

Sasaran diatas, jika dapat dicapai, akan memberikan manfaat kepada perusahaan dalam menjaga keamanan informasinya. Manfaat yang diharapkan dari pencapaian sasaran ini sebagai berikut:

- Memberikan arahan tentang pengelolaan keberlansungan bisnis di perusahaan yang perlu dibangun.
- Perusahaan akan memiliki rancangan penanggulangan bencana, untuk tetap menjaga jalannya bisnis bisa terus berlangsung, saat terjadi bencana.

6.5 Strategi

Strategi keamanan informasi merupakan bagian penting dari rancangan 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.

Tabel 6.5 Tujuan , Sasaran dan Strategi

Goals	Objective	Strategy			
		1	2	3	4
Prevent	Dapat menentukan kebijakan yang dibutuhkan dalam mendukung implementasi keamanan informasi.	√			
	Dapat mengidentifikasi kebutuhan Sumber Daya Manusia (SDM) dalam mendukung keamanan informasi	√	√		
	Dapat mengidentifikasi pembangunan pemeliharaan sistem, yang perlu dilakukan.	√		√	√
Reduce	Dapat mengidentifikasi aset-aset perusahaan yang kritikal milik perusahaan, serta mengidentifikasi risiko, ancaman dan kerawanannya.	√			
	Dapat mengidentifikasi insiden keamanan informasi yang berpotensi terjadi.	√		√	√
	Dapat mengidentifikasi pengelolaan fisik dan lingkungan keamanan informasi.	√		√	√
	Dapat mengidentifikasi pengelolaan komunikasi dan operasional keamanan informasi.	√	√		
Respond and Recover	Dapat melakukan audit dan korektif terhadap kesalahan atau gangguan yang terjadi.	√		√	√
	Dapat mengidentifikasi pengelolaan keberlanjutan bisnis, yang perlu dilakukan.	√			√

Empat strateg diatas, diperoleh dari hasil tahapan *risk mitigation* yang telah dilakukan, yang bertujuan untuk menurunkan risiko yang berpotensi dapat terjadi. Upaya untuk menurunkan risiko tersebut, sudah merupakan tujuan dan sasaran dari rancangan keamanan informasi. Penjelasan setiap strategi, akan dibahas pada bagian selanjutnya.

6.5.1 Strategi: Menyusun kebijakan, prosedur dan standard

Strategi yang pertama ialah menyusun kebijakan, prosedur dan standard terkait dengan keamanan informasi. Strategi ini dijalankan dengan melakukan beberapa aksi atau kegiatan untuk dapat menjalankan strategi diatas, sebagai berikut:

1. Melakukan identifikasi terhadap kebijakan, prosedur dan standard yang penting untuk disusun dan ditetapkan
2. Melakukan identifikasi informasi yang sensitif, untuk menetapkan kebijakan, prosedur dan standard dalam penggunaan dan pengelolaan informasi tersebut.
3. Memilih tempat dan lokasi penyimpanan data backup yang terpisah dari ruang data center, yang akan dijadikan kebijakan.

6.5.2 Strategi: Memperbaiki pola rekruitmen dan pelatihan SDM TI

Strategi yang kedua ialah menyempurnakan pola rekuitmen dan pelatihan SDM TI. Strategi ini dijalankan dengan melakukan beberapa aksi atau kegiatan untuk dapat menjalankan strategi diatas, sebagai berikut:

1. melakukan pemeriksaan latar belakang dari calon karyawan TI.
2. melakukan penyesuaian kontrak perjanjian kerja dengan kebijakan pemerintah dan perusahaan, untuk selanjutnya menjalankannya secara disiplin.
3. melakukan pembinaan dengan melaksanakan pelatihan tentang kepedulian menjaga keamanan informasi.
4. Memberikan penugasan dan memperhatikan sharing responsibilities, berdasarkan beban kerja dan kompetisi, agar pekerjaan dalam menjaga keamanan informasi dapat secara disiplin dijalannkan dengan penuh tanggung jawab.

6.5.3 Strategi: Mengimplementasikan perangkat preventive dan detection

Strategi yang ketiga ialah mengimplementasikan perangkat preventive dan detection terhadap serangan dan gangguan keamanan informasi. Strategi ini dijalankan dengan melakukan beberapa aksi atau kegiatan untuk dapat menjalankan strategi diatas, sebagai berikut:

1. Melakukan scanning virus secara teratur, serta memperbaharui perangkat anti virus secara berkala.
2. Melakukan pemasangan anti petir dan grounded yang tahan terhadap petir berintensitas besara, yang biasa di lokasi kantor.
3. Melakukan implementasi firewall, yang bertujuan melindungi server dalam daerah DMZ, terhadap serangan yang bisa berasal dari dalam.
4. Mengimpelemtasikan aplikasi intrusion detection system (IDS), untuk mendeteksi serangan dan gangguan keamanan yang menyerang sistem.
5. Menggunakan enkripsi pada informasi yang dianggap sangat rahasia.
6. Melakukan pembatasan fungsi dan informasi kepada user dengan otoritas yang telah ditetapkan.

6.5.4 Strategi:Menerapkan pola pemeriksaan dan evaluasi operasiona TI

Strategi yang keempat ialah menerapkan pola pemeriksaan dan evaluasi operasional TI terkait keamanan informasi. Strategi ini dijalankan dengan melakukan beberapa aksi atau kegiatan untuk dapat menjalankan strategi diatas, sebagai berikut:

1. Melakukan peningkatan kegiatan pengawasan terhadap kerja dari para operator yang berjumlah cukup banyak, agar terkelola autentifikasi dan otoritas yang telah diberikan.
2. Melakukan pertukaran perkejaan di divisi TI, agar tidak ada seorang personil yang menguasai satu kritikal teknologi.
3. Melakukan *call back system*, untuk memversifikasi perubahan data dan kesalahan yang dilakukan pada proses input data, yang dapat menyebabkan kesalahan kirim dan penempatan barang.
4. Mencatat kejadian berupa gangguan atau serangan terhadap sistem TI yang berpotensi besar terjadi kembali.

6.6 Kontrol Keamanan

Tujuan rancangan 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.

Rekomendasi aksi tersebut akan mengimplementasikan kontrol-kontrol keamanan sesuai dengan strategi yang akan dicapai. Kontrol keamanan merupakan kebijakan, prosedur, kebiasaan dan struktur organisasi yang dirancang untuk menjamin bahwa tujuan-tujuan bisnis dapat tercapai; sedangkan insiden yang merugikan dapat dicegah, dideteksi dan dikoreksi.

Adapun kontrol keamanan tersebut, sebagai berikut:

Tabel 6.6 Strategi dan Kontrol Keamanan

No	Strategy	No	Securirty Control
1	Menyusun kebijakan, prosedur dan standard terkait dengan keamanan informasi	1	Kebijakan dan prosedur,
		2	Labeling of sensitive material
		3	Penyimpanan backup data pd tempat aman
2	Menyempurnakan pola rekruitmen dan pelatihan dan pengelolaan SDM TI	4	Pemeriksaan latar belakang
		5	Perjanjian kerja
		6	Pelatihan security awarness
		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 gound
		12	Pemasangan firewall
		13	Intrusion Detection System.
		14	Enkripsi
		15	Pembatasan fungsi dan informasi
		16	Penggunaan call back system
4	Menerapakan pola pemeriksaan dan evaluasi operasional TI terkait keamanan informasi	17	Violation report
		18	Audit trail information

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

Hasil penilaian delapan aspek penilaian risiko diatas, menghasilkan kelemahan/kerawanan dan ancaman, yang menjadi kumpulan risiko. Setiap risiko akan dinilai kecenderungan dan dampaknya, yang akan 'memberikan nilai risiko. Nilai risiko tersebut akan dikategoterikan menjadi "*high*", "*medium*" atau "*low*". Kumpulan risiko dan tingkatannya selanjutnya dijadikan dasar dalam merekomendasikan kontrol keamanan yang dapat mencegah atau menurunkan risiko tersebut, sehingga proses penilaian risiko akan menghasilkan dua hal, yaitu :

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

Selanjutnya dilakukan tahapan risk mitigation, atau upaya untuk memitigasi risiko. Proses yang dilakukan dalam tahapan ini ialah melakukan penentuan aksi mitigasi yang dilanjutkan dengan evaluasi, analisis cost-benefit, analisis cost-effectiveness.terhadap rekomendasi kontrol yang terkait dengan prioritas aksi yang harus dilakukan untuk mitigasi risiko. 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 akan 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. Hasi analisis ini akan menjelaskan manfaat dan kerugian, jika kontrol ini diimplementasikan atau tidak diimplemntasikan, sehingga menjadi pertimbangan bagi perancangan keamanan informasi.
d. Hasil analisis *cost-effectiveness* terhadap kontrol keamanan yang direkomendasikan. Hasil analsisi ini akan 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. Rancangan kontrol keamanan, yang berisi tentang keburuhan sumber daya yang harus disiapkan untuk mengimplementasikan kontrol-kontrol keamanan tersebut, serta tim yang dibentuk untuk mengimplementasikannya.

Rancangan keamanan yang komprehensif telah disusun, berdasarkan tahapan penilaian risiko (*risk assessment*) dan risk mitigation, sehingga secara lengkah memberikan pertimbangan dan dasar dalam menentukan tujuan, sasaran, startegi dan kontrol keamanan untuk menjamin keamamann informasi di PT. Multi Terminal Indonesia.

6.7 Rancangan Implementasi Kontrol Keamanan

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

Tabel 6.7 Rancangan Implementasi Kontrol

No	Security Control	Management Control	Technical Control	Opertional Control
1	Kebijakan dan prosedur,	√		
2	Labeling of sensitive material	√		
3	Penyimpanan backup data pd tempat aman			√
4	Pemeriksaan latar belakang	√		
5	Perjanjian kerja	√		
6	Pelatihan security awarness	√		
7	Sharing responsibilities	√		
8	Scanning terhadap virus		√	
9	Pemasangan anti petir dan gound			√
10	Pemasangan firewall	√		
11	Intrusion Detection System.		√	
12	Enkripsi		√	
13	Pembatasan fungsi dan informasi		√	
14	Increased supervisions	√		
15	Job rotation	√		
16	Penggunaan call back system		√	
17	Violation report	√		
18	Audit trail information	√		

6.7.1 Rancangan Implementasi Kebijakan Keamanan Informasi

Terdapat langkah-langkah dalam mengimplementasi kebijakan keamanan informasi oleh perusahaan:

1. Persiapan
    a. Menyusun kebijakan keamanan informasi
    b. Menetukan standard
    c. Menentukan guidelines
    d. Menyusun prosedur
    e. Menentukan tim pelaksana
2. Implementasi
    a. Menanamkan kepedulian akan kebijakan keamanan informasi
    b. Memelihara kepedulian tersebut
3. Review and Evaluasi

Kebijakan yang harus disusun, diperoleh dari hasil analisis pada tahapan risk mitigation, yang bersumber pada tahap penilaian risiko, adapun kebijakan tersebut antara lain:

- Kebijakan Klasifikasi Informasi
- Kebijakan Dekstop
- Kebijakan Pencatatan Kejadian Gangguan Keamanan dan TI
- Kebijakan Ruang DRC
- Kebijakan Pembuatan BCP dan DRP
- Kebijakan Pemasangan Anti petir dan grounded
- Kebijakan Integrasi Sistem Aplikasi
- Kebijakan untuk mengukur Kinerja dan beban sistem
- Kebijakan Firewall pada jaringan lokal
- Kebijakan Pencegahan Penyebaran Virus
- Kebijakan tentang aktivitas pemeliharaan perangkat pendukung

Dokumen standard akan menjelaskan spesifik teknologi yang harus digunakan dalam menjaga keamanan informasi. Sedangkan standard yang harus juga dibangun oleh perusahaan, antara lain:

- Standard dalam pengklasifikasian informasi
- Standard peralatan dan perlengkapan ruang DRC.
- Standard peralatan anti petir dan grounded
- Standard keamanan aplikasi bisnis
- Standard perangkat anti virus

Dokumen guidelines, digunakan untuk merinci standard yang telah ditentukan. Guidelines akan lebih fleksibel dibandingkan standard. Perusahaan membutuhkan dokumen guidelines, antara lain:

- Guidelines dalam pencatatan gangguan keamanan informasi.
- Guidelines dalam penyusunan BCP dan DRP
- Guidelines dalam pengukuran kinerja dan beban sistem
- Guidelines scanning virus
- Guidelines pelabelan informasi yang sensitif.

Dokumen prosedur dapat menjelaskan langkah-langkah dalam melakukan kegiatan atau tugas tertentu. Perusahaan perlu menyusun prosedur untuk memberikan panduan dalam pelaksanaan suatu tugas. Prosedur tersebut antara lain:

- Prosedur pengiriman dan pengelolaan informasi yang kritikal
- Prosedur dalam pencegahan penyebaran virus komputer.
- Prosedur dalam mengaktifkan fitur keamanan pada desktop.

Penentuan tim pelaksana, dapat dilakukan dengan membentuk tim dengan kemampuan sebagai berikut:

- memiliki otorisasi dalam melakukan review dan penelitian tentang materi kebijakan yang akan ditetapkan.
- Memiliki otoritas dalam mendorong agar kebijakan tersebut dapat dijalankan oleh perusahaan.

Kebijakan yang telah disusun dan ditetapkan tidak akan berjalan, tanpa ada kegiatan untuk mendorong implementasi kebijakan berhasil. Kegiatan yang harus dilakukan agar kebijakan dapat berjalan secara efektif, ialah:

- Menanamkan kepedulian akan keamanan informasi.
- Memelihara kepedulian tersebut tetap dimiliki oleh pimpinan dan karyawan perusahaan.

Untuk menanamkan kebijakan keamanan informasi berikut ini cara yang harus dilakukan oleh perusahaan:

- Memberi pengumuman tentang isi kebijakan keamanan informasi tersebut, dalam bentuk elektronik dan kertas.
- Mengadakan pelatihan atau workshop tentang keamanan informasi
- Menyapaikan kepada karyawan baru atau pengguna baru.

Sedangkan dalam untuk memelihara kepedulian yang telah dimiliki oleh pimpinan dan karyawan, dapat dilakukan dengan cara, antara lain:

- Menampilkannya secara rutin dan bervariasi pada website/portal internal milik perusahaan.
- Penyampain yang terus menerus melalui poster, email atau lembaran.

Kebijakan yang telah ditetapkan, dan disosialisasikan, perlu direview dan dievaluasi efektivitasnya dan keseusian terhadap kerawanan/kelemahan yang akan dikurangi. Hal ini dapat dilakukan dengan beberapa kegiatan, antara lain:

- Menunjuk perseorangan atau tim untuk melakukan review dan evaluasi terhadap kebijakan keamanan informasi.
- Menganalisis laporan insiden yang tercatat, sejak diterapkannya kebijakan keamanan informasi, sehingga akan terlihat dampak penerapan kebijakan terhadap jumlah insiden/kejadian gangguan keamanan informasi.

6.7.2 Rancangan Implementasi Pelabelan informasi sensitif

Pelabelan informasi sensitif (*labeling of sensitive material*), merupakan upaya untuk membangun keamanan informasi elektronik dan fisik. Langkah-langkah dalam menjaga keamanan informasi sensitif, sebagai berikut:

1. Pengiriman informasi harus diklasifikasi berdasarkan sensitifitasnya, sehingga menggunakan perlindungan informasi.
2. Menjalankan prosedur untuk melindungi informasi dari modifikasi dan serangan terhadap layanan dan ketersediaan informasi dari pihak yang tidak berhak.
3. Memastikan bahwa pengguna informasi yang terhubung dengan jaringan komputer merupakan pihak yang memiliki otorisasi.

6.7.3 Rancangan Implementasi Penyimpanan backup data pada tempat aman

Backup harus dilakukan berdasarkan prosedur yang disusun secara baik, untuk melakukan backup dan melindungi hasilnya. Dalam melakukan backup terdapat prosedur sebagai berikut:

1. Mengetahui bagian data yang penting dan skala waktu untuk melakukan backup.
2. Melakukan prosedur backup dengan panduan yang diberikan oleh perangkat backup yang digunakan.
3. Melatakkan hasil backup pada tempat yang aman, yang terpisah dari tempat data center.

6.7.4 Rancangan Implementasi Pemeriksaan latar belakang

Pemeriksaan latar belakang dari calon karyawan tidak hany untuk memperoleh kompetensi dan keahlian yang sesuai dengan kebutuhan, tetapi untuk mengetahui kejadian yang pernah dialaminya di tempat pekerjaan sebelumnya. Pemeriksaan ini dilakukan dengan langkah-langkah di bawah ini:

1. Melakukan verfikasi atas data yang disertakan oleh calon karyawan tersebut, seperti referensi tentang karakter, pelatihan yang pernah diikutinya, pengalaman profesional dan akademik, serta keberhasilan dan kegagalan yang pernah diperolehnya.
2. Melakukan pengecekan kembali, saat seorang karyawan akan berpindah divisi atau mendapatkan promosi jabatan.

6.7.5 Rancangan Implementasi Perjanjian Kerja

Perjanjian kerja harus mengatur tentang hak dan kewajiban perusahaan dan pegawai baru. Hal ini bertujuan untuk memberikan kepastian karir kepada pegawai baru, dan aturan dalam menjalankan pekerjaannya, termasuk kewajiban untuk menjaga keamanan informasi perusahaan. Langkah-langkah dalam penerapan perjanjian kerja, sebagai berikut:

1. Persiapan
    - Perusahaan dan Serikat Kerja mempersiapkan data dan informasi, terkait dengan hak dan kewajian perusahaan dan karyawan, yang dituntut kedua belah pihak dan Undang-Undang terkait dengan Ketenagakerjaan.
2. Perundingan dan Penyusunan Perjanjian Kerja
    - Perusahaan dan Serikat kerja melakukan perundingan mengenai hak dan kewajiban, gaji, dan waktu kontrak, serta karir yang akan diberikan perusahaan kepada karyawan.
3. Penandatanganan dan Pelaksanaan Perjanjian Kerja
    - Melakukan sosialisasi dan implementasi perjanjian kerja kepada para karyawan, dengan tujuan memberikan kepastian karir dan menegaskan kewajiban karyawan dan perusahaan dalam menjaga keamanan infromasi milik perusahaan.

6.7.6 Rancangan Implementasi Pelatihan Security Awarness

Dalam melakukan pelatihan kepada pengguna aplikasi dan informasi, perlu dipersiapkan beberapa hal, antara lain:

1. Membangun aturan dan regulasi akses informasi, bagi pengguna dan divisi yang bertanggungjawab.
2. Melakukan pelatihan kepada seluruh pengguna tentang cara pengaksesan informasi dan sistem dengan aman, sesuai prosedur dan kebijakan.
3. Pelatihan kepadulian keamanan informasi, berisi tentang:
   - Hal yang boleh dan tidak boleh dalam proses akses informasi tau aplikasi
   - Cara melaksanakan dan menggunakan kontrol akses dan menjalankan tanggungjawab
   - Cata melaksanakan prosedur untuk melaporkan kejadian/insiden yang mengganggu keamanan informasi.

6.7.7 Rancangan Implementasi Sharing Responsibility

Pembagian tanggung jawab pada divisi TI di perusahaan perlu dilakukan, karena terdapat tugas yang kritikal yang harus dilakukan dan diperhatikan secara baik oleh penanggungjawab TI.

1. Melakukan identifikasi beban kerja setiap karyawan pada divisi TI.
2. Mengidentifikasi tugas-tugas kritikal yang perlu dibagi pada setiap posisi di divisi TI.
3. Melakukan evaluasi pelaksanaan tanggungjawab yang diberikan, terutama tugas-tugas kritikal.

Salah satu tugas kritikal yang perlu diperhatikan dalam penugasan dan pembagian kerja, jika petugas berhalangan di PT.Multi Terminal Indonesia ialah melakukan test terhadap hasil backup. Tugas pengujian backup dilakukan dengan prosedur sebagai berikut:

1. Menguji hasil file backup secara berkala, untuk memastikan data berhasil di restore.
2. Menguji prosedur pemulihan data, untuk memastikan prosedur backup mampu mengurangi risiko kegagalan backup data.

6.7.8 Rancangan Implementasi Scanning terhadap virus

Scanning terhadap virus, tidak terlepas dari serangan malicious software, seperti *network worms, trojan horses, logic bombs*. Adapun guidelines untuk mengimplementasika sebagai berikut:

1. Menggunakan software yang berlisensi untuk OS dan perangkat lunak lainnya.
2. Menghindari file dari sumber yang tidak jelas.
3. Melakukan update terhadap perangkat lunak antivirus yang digunakan secara teratur.
4. Memperhatikan *warning* atau peringatan yang berasal dari perangkat antivirus saat menjalankan aplikasi.

6.7.9 Rancangan Implementasi Pemasangan anti petir dan grounded

Anti petir dan gounded yang tidak handal, dapat berisiko besar terhadap keamanan informasi, karena akan menyebabkan kerusakan server dan peralatan jaringan komputer, seperi switch. Hal yang harus diperhatikan dalam pemilihan perangkat anti perit dan grounding

1. Melakukan pemeriksaan terhadap anti petir sebelumnya, untuk menemukan kelemahan dalam menangkal petir dalam pengamanan gedung.
2. Petir tidak hanya mengenai gedung, tetapi arus petir yang sering merusak server dan peralatan jaringan, berasal dari petir yang mengenai jaringan listrik dan arus petir ini masuk ke bangunan miliki perusahaan mengikuti kabel listrik dan merusak panel, sehingga yang dipelukan ialah memasang perangkat arrester (penahan surya atau pelepas tegangan lebih).
3. Melakukan evaluasi terdapat penggunaan anti petir dan penurun tegangan lebih.

6.7.10 Rancangan Implementasi Pemasangan Firewall

Implementasi *firewall* memiliki langkah-langkah sebagai berikut:

1. Menyusun kebijakan keamanan informasi terkait pilihan arsitektur firewall. Terdapat pilihan arsitektur firewall untuk perusahaan, antara lain single firewall behind DMZ, single firewall in front of DMZ, atau dual or multitier firewall
2. Memilih komponen firewall.
3. Melakukan desain berdasarkan pilihan arsitektur dan komponen firewall yang digunakan.

4. Implementasi firewall dan konfigurasi.
5. Melakukan review dan testing terhadap firewall yang sudah diimplementasi.

6.7.11 Rancangan Implementasi IDS

Untuk mengimplementasikan kontrol ini, memiliki tahapan sebagai berkut:

1. Menyusun kebijakan untuk menentukan pendekatan yang akan digunakan dalam mengimplementasikan IDS. Terdapat pendekatan dalam mengimplementasikan IDS, antara lain Host Monitoring System , Host-based IDS dan Host-nased Network IDS.
2. Pemilihan paket teknologi IDS yang ditawarkan oleh vendor IDS.
3. Perancangan IDS pada lingkungan jaringan komputer perusahaan.
4. Implementasi dan Evaluasi IDS pada perusahaan.

6.7.12 Rancangan Implementasi Enkripsi

Implementasi teknik enkripsi dilakukan dengan langkah-langkah sebagai berikut:

1. Membangun kebijakan untuk mengelola kunci kriptografi elektronik, beberapa kunci enkripsi, antara lain: *symmetric*, *public* dan *private*.
2. Melindungi kunci dari modifikasi dan kerusakan.
3. Memastikan bahwa pengelolaan kunci enkripsi, mengacu pada standard keamanan yang berlaku.
4. Kebijakan pengelolaan kunci, harus mengandung hal-hal di bawah ini:
    - Melakukan *generate key* dari sistem *cryptografi* yang berbeda dan aplikasi yang berbeda.
    - Menggunakan public key certificate.
    - Menyimpan kunci pada tempat yang aman.

6.7.13 Rancangan Implementasi Pembatasan fungsi dan informasi

Pembatasan fungsi dan informasi bertujuan untuk memberikan fungsi dan informasi sesuai dengan otoritas dan kebutuhan dari pengguna, sehingga pengguna hanya akan menggunakan fungsi dan mengakses informasi sesuai dengan otoritasnya. Langkah-langkah implementasi pembatasan fungsi dan informasi sebagai berikut:

1. Melakukan identifikasi terhadap pengguna dan tugas-tugasnya terhadap fungsi di aplikasi dan informasi.
2. Melakukan custimizition terhadap aplikasi, untuk menyesuaikan fungsi dan informasi yang digunakan oleh pengguna, agar sesuai dengan otoritas yang diberikan, berdasarkan pekerjaan dan tugasnya.
3. Melakukan evaluasi terhadap perubahan tugas dan pekerjaan pengguna.

6.7.14 Rancangan Implementasi Increased supervision

Peningkatan pengawasan terhadap kerja para karyawan, dalam upaya menjalankan kebijakan dan prosedur untuk menjaga keamanan informasi, perlu dilakukan oleh peruhsaan. Hal ini disebabkan oleh jumlah user/pengguna aplikasi dan informasi di PT.Multi Terminal Indonesia cukup banyak, sehingga harus diimbangi dengan peningkatan pengawasan, agar tidak terjadi kecerobohan atau hilangnya keamanan informasi.

Adapun langkah-langkah dalam meningkatkan pengawan ini, antara lain:

1. Menentukan kritikal aspek yang harus menjadi perhatian pengawasan, berdasarkan tingkat risiko pada proses penilaian risiko.
2. Memperhatikan kebijakan dan prosedur sebagai acuan dalam melakukan pengawasan.
3. Melakukan pencatatan terhadap hasil pengawasan, dan pelaporan.

6.7.15 Rancangan Implementasi Job rotation

Job rotation akan sesuai diimplementasikan pada lingkungan pekerjaan yang kritikal terhadap jalannya bisnis perusahaan. Hal ini dilakukan untuk menurunkan risiko pekerjaan kritikal tersebut hanya dikuasai oleh satu individu dalam divisi tersebut, sehingga perlu dilakukan rotasi pekerjaan antar karyawan yang ada di divisi TI pada perusahaan. Langkah-langkah dalam implementasi job ratation, sebagai berikut:

1. Membuat kebijakan mengenai rotasi pekerjaan, yang akan menentukan beberapa hal, antara lain:
    a. Menetukan banyaknya titik pekerjaan yang akan dirotasi.
    b. Menetukan frekuensi dilakukannya rotasi pekerjaan.
    c. Administrasi perintah rotasi pekerjaan pada karyawan.
    d. Menyiapkan anggaran untuk gaji pegawai
2. Implementasi rotasi pekerjaan, dengan
    4. Melakukan pelatihan terhadap karyawan dengan posis pekerjaan yang baru, harus disiapkan oleh perusaan.
3. Review dan Evaluasi dari kegiatan rotasi pekerjaan.

6.7.16 Rancangan Implementasi Penggunaan call back system

Call back system merupakan aktivitas untuk menghubungi pengguna informasi atau aplikasi, yang melakukan perubahan terhadap informasi tertentu. Implementasi kontrol ini digunakan untuk mencegah perubahan dan akses pada file atau sistem terkait dengan informasi sensitif.

Adapun tahapan dalam mengimplementasi *call back system*, sebagai berikut:

1. Menyusun prosedur dalam melakukan call back system, antara petugas dengan pusat pemantau, dan sebaliknya.

2. Menyiapkan peralatan komunikasi bagi setiap petugas di lapangan, agar dapat berkomunikasi dengan pusat pemantau.
3. Melakukan pencatatan terhadap perubahan dan akses data yang tidak biasa dalam sebuah laporan, jika ditemukan kesalahan entry data.

6.7.17 Rancangan Implementasi Violation report

Pembuatan laporan atas kejadian/insiden gangguan atau serangan terhadap keamanan informasi, harus tercatat secara sistematik berdasarkan kronologi kejadian tersebut. Violation report minimal harus mengadung informasi sebagai berikut:

- Tipe Insiden (*incident type*)
- Tingkat kekuatannya serangan (*severity level*)
- Pintu akses yang digunakan
- Keterlibatan

Dalam melakukan implementasi violation report terdapat langkah-langkah sebagai berikut:

1. Menyusun metode atau teknik untuk pencatatan dan hal yang spesifik pada sebuah kejadian/insiden, untuk dapat mengenalai dan melakukan pelacakan.
2. Membuat prosedur jika terjadi peningkatan kejadian/insiden keamanan informasi ke administrator atau management.

6.7.18 Rancangan Implementasi Audit trail

Salah satu hal penting dalam keamanan informasi ialah dapat menjamin prinsip *accountability*, yaitu kemampuan untuk mengetahui aksi dan perilaku dari individu dalam menggunakan sistem, dan untuk mengidentifikasi fakta-fakta yang terjadi pada sistem dan informasi.

Terdapat tiga hal pada audit trail yang dapat diimplementasi

1. Melakukan pencatatan aksi dalam sebuah dokumen
   - Mencatat individu yang mengakses dan merubah informasi dalam sistem atau dokumen tertentu.
   - Mencatat frekuensi diaksesnya sebuah informasi oleh pengguna
2. Melakukan pencatatan lanjutan
   - Mencatat permintaan user untuk mencetak informasi, mengirimkan informasi digital dan dokumen.
   - Mencatat pencobaan dalam perubahan password.