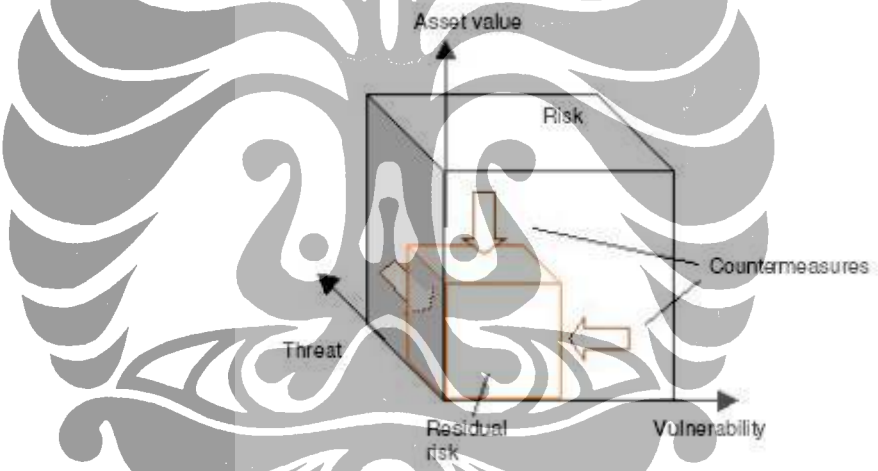
BAB 2 TINJAUAN TEORI

2.1 Teori Risiko

Yulianto (2006) menyatakan bahwa risiko merupakan sesuatu yang akan terjadi, dipengaruhi oleh faktor kemungkinan (*likelihood*), berupa ancaman (*thread*) terhadap beberapa kelemahan (*vulnerabilities*) yang menghasilkan dampak (*impact*) yang merugikan organisasi. Sedangkan pengamanan informasi dan sistem informasi adalah perlindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak terotorisasi.



Gambar 2.1 Hubungan risiko, ancaman, kerawanan, dan nilai aset

Ancaman (*threat*) adalah sesuatu yang dapat menganggu kegiatan organisasi. Kerawanan/kelemahan (*vulnerability*) adalah potensi kegagalan atau kelemahan yang menyebabkan risiko. Kecenderungan (*likelihood*) adalah kemungkinan terjadinya suatu risiko. Dampak (*impact*) adalah kerusakan atau efek yang dialami organisasi akibat terjadinya risiko.

Soohoo(2005) mengklasifikasikan risiko menjadi beberapa jenis, sebagai berikut;

a. Risiko spekulatif *(speculative risk)*
b. Risiko murni *(pure risk*)
c. Risiko fundamental *(fundamental risk*)
d. Risiko khusus *(particular risk)*

Adapun penjelasan dari tiap jenis klasifikasi risiko, akan dijelaskan seperti di bawah ini:

- Risiko spekulatif *(speculative risk)*adalah risiko yang memberikan kemungkinan keuntungan (*gain*) atau kerugian (*loss*) atau tidak untung atau tidak rugi (*break even*). Risiko spekulatif disebut juga risiko dinamis (*dynamic risk*). contohnya adalah risiko dalam dunia perdagangan.
- Risiko murni *(pure risk)* adalah risiko yang hanya mempunyai satu akibat yaitu kerugian, sehingga tidak ada orang yang menarik keuntungan dari risiko ini. Contohnya adalah gempa bumi dan banjir (*natural disaster*).
- Risiko fundamental *(fundamental risk)* adalah risiko yang sebab maupun akibatnya impersonal (tidak menyangkut seseorang), dimana kerugian yang timbul dari risiko yang bersifat fundamental biasanya tidak hanya menimpa seseorang individu melainkan menimpa banyak orang. Contohnya adalah *natural disasater* atau perang, inflasi (*sosial phenomenon*).
- Risiko khusus *(particular risk)* adalah risiko khusus yang disebabkan oleh peristiwa-peristiwa individual dan akibatnya terbatas. Contohnya adalah pencurian.

Terdapat empat klasifikasi risiko lainnya, yaitu hazard *risk, financial risk, strategy risk* dan *operational risk*, dengan penjelasan sebagai berikut:

- Risiko tidak dapat dihindari *(hazard risk)*, contohnya kebakaran, banjir, pencurian.
- Risiko keuangan *(financial risk)*, contohnya inflasi, harga, kredit
- Risiko strategi *(strategy risk)*, contohnya kompetisi, inovasi teknologi, perubahan regulasi.
- Risiko operasional *(operational risk)*, contohnya keamanan terhadap ancaman, keamanan IT, operasi bisnis.

Tremper (2005) dalam artikelnya yang berjudul "*How to Develop a Risk Management Plan*", menyatakan fungsi umum yang biasa digunakan dalam menghitung risiko adalah:

RISK = Probability x Impact

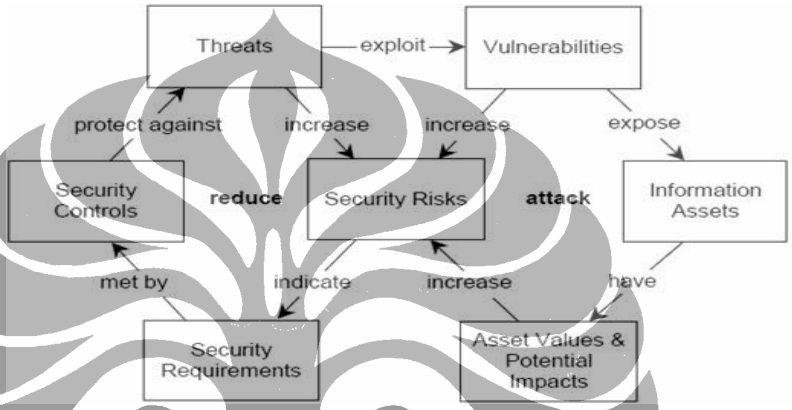
Keterangan:

- *Probability* ialah ukuran kemungkinan suatu kejadian
- *Impact* adalah ukuran dampak jika hal tersebut terjadi.

Klasifikasi ancaman yang telah diuraikan diatas,sangat terkait dengan keamanan informasi dan data, agar tidak mengalami gangguan keamanan, seperti di bawah ini:

- Kehilangan kerahasiaan informasi *(loss of confidentiality of information)*, bahwa informasi diperlihatkan kepada pihak yang tidak berhak untuk melihatnya.
- Kehilangan keutuhan informasi *(loss of integrity of information)*, bahwa informasi tidak lengkap, tidak sesuai aslinya, atau telah dimodifikasi secara ilegal.
- Ketidaktersediaan informasi *(loss of availability of information*, bahwa informasi tidak tersedia saat dibutuhkan.

Pada panduan ISO 27001 tentang *Information Security Management System* (ISMS), digambarkan bahwa resiko keamanan dapat meningkat sesuai dengan banyaknya ancaman, yang teridentifikasi. Ancaman tersebut akan memanfaatkan kelemahan/kerawanan setiap aset atau proses pada organisasi, dan hanya dapat dikurangi dengan digunakan kontrol keamanan (*security control*), dimana kontrol keamanan tersebut dapat diperoleh dari hasil identifikasi kebutuhan keamanan yang dilakukan. Kebutuhan keamanan muncul berdasarkan identifikasi risiko keamanan.



Gambar 2.2 Risk Diagram

Resiko keamanan juga dapat meningkat karena disebabkan oleh adanya kelemahan/kerawanan dan dampak potensial. Kelemahan/kerawanan dimiliki oleh setiap aset organisasi, yang jikalau aset tersebut terganggu, maka akan menimbulkan kehilangan nilai pada aset tersebut, dan dampak yang potensial terjadinya tinggi, yang dapat menimbulkan resiko keamanan. Untuk itu perlu dilakukan suatu pengelolaan risiko, dengan tujuan dapat mengurangi risiko yang dapat menganggu jalannya bisnis. Pengelolaan risiko akan dijelaskan selanjunya.

2.2 Pengelolaan Risiko (*Risk Management*)

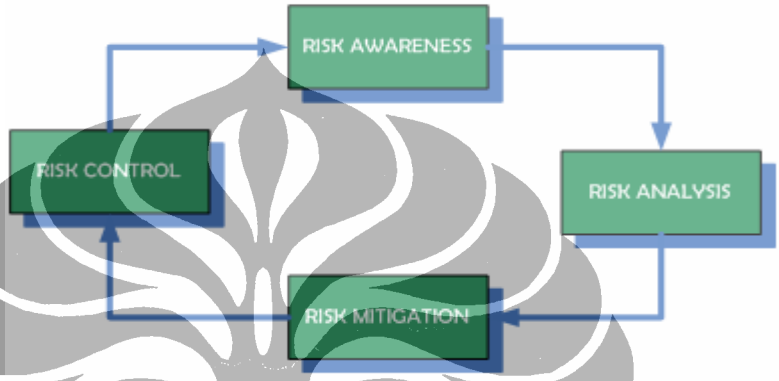
Valerdi (2004) menjelaskan bahwa pengelolaan risiko ialah proses untuk mengidentifikasi kerawanan/kelemahan (*vulnerability)* dan ancaman (*threats*) terhadap aset informasi yang dimiliki oleh perusahaan dalam mencapai tujuan dan sasaannya, dan dengan tujuan utamanya adalah mengurangi risiko terhadap keamanan sistem dan data.

Pengelolaan risiko akan sangat efektif, jika perusahaan yang memiliki aset informasi, telah menyadari pentingnya, mengurangi risiko yang mungkin akan dihadapi, dan dapat mengganggu kinerja perusahaan. Kesadaran tersebut, akan dapat mendorong dilakukannya pengelolaan risiko, yang berdampak pada peningkatan biaya yang harus dikeluarkan, untuk melindungi seluruh aset informasi yang penting bagi perusahan.

Pada pengelolaan risiko dilakukan identifikasi atau klasifikasi informasi atau aset sensitif dan kritikal, dari kerawanan/kelemahan (*vulnerability)* dan ancaman (*threats*), yang dimilikinya. Tujuan dari klasifikasi diatas, adalah untuk menentukan prioritas objek yang akan diteliti, dan menentukan cara untuk melindungi aset tersebut. Contoh dari aset perusahaan yang harus dilindungi, meliputi informasi atau data, perangkat keras dan perangkat pendukung, perangkat lunak, layanan (*services*), arsip atau dokumen, dan personil.

Terdapat beberapa ancaman (*threats*) yang mungkin akan dihadapi dalam upaya menjaga keamanan aset. Adapun ancaman tersebut, antara lain *error, malicious damage/attack, froud, theft dan equipment/software failure*. Ancaman tersebut timbul disebabkan adanya *vulnerabiliy,* yang dapat membuka peluang terjadinya ancaman. Contoh dari *vulnerability*, antara lain *lack of user knowledge, lack of security functionality, poor choice of password, untested technology, transmission of unprotected communication*.

Rekomendasi yang akan dihasilkan dari adanya pengelolaan risiko ini ialah, pertama tersusunnya sebuah kebijakan perusahaan (*organizational policy*) terkait dengan keamanan aset informasi. Kedua, hasil identifikasi dan pengukuran tingkat risiko dapat memberikan informasi tingkat risiko TI yang harus diperhatiankan oleh perusahaan, khususnya departemen/divisi TI. Ketiga, diperolehnya rincian biaya dan efektivitas untuk implementasi.



Gambar 2.3*Risk Management Life Cycle*

Enisa (2006) menjelaskan bahwa pada daur hidup pengelolaan risiko, dibutuhkan suatu kesadaran akan risiko (*risk awarness*) yang akan mendorong dilakukannya analisis terhadap risiko. Kesadaran akan risiko, yang berpotensi terjadi, harus dimiliki oleh beberapa level yang ada di perusahaan, antara lain:

- Level Operational, dimana pada level ini, kesadaran akan pengelolaan risiko TI dilakukan dengan menjaga efektivitas penggunaan sistem TI dan infrastrukturnya yang sesuai dengan prosedur kerja yang telah ditetapkan.
- Level Proyek: pada level ini, kesadaran akan pengelolaan risiko TI dilakukan dengan mengelola kompleksitas proyek-proyek yang dikerjakannya, agar tidak menimbulkan risiko yang akan menyebabkan gagalnya penyelesaikan proyek.
- Level Strategik, dimana pada level ini, kesadaran akan pengelolaan risiko TI dilakukan dengan tetap menjaga keselarasan (*alignment*) antara portofolio aplikasi dan TI, dengan strategi bisnis perusahaan, agar terhindar dari kesenjangan yang sangat jauh antara kebutuhan dan dukungan perangkat yang dimiliki.

Terdapat dua pendekatan dalam melakukan pengelolaan risiko, yaitu pendekatan berdasarkan aset, dan pendekatan berdasarkan proses bisnis organisasi, dengan penjelasan sebagai berikut:

- Pendekatan berdasarkan aset, yaitu pendekatan ini melakukan pengelolaan risiko dengan berdasarkan identifikasi kritikal aset, dan risiko-risiko yang dapat terjadi pada aset tersebut.
- Pendekatan berdasarkan proses bisnis, yaitu pendekatan ini melakukan pengelolaan risiko dengan berdasarkan identifikasi proses bisnis yang kritikal pada organisasi, dan risiko-risiko yang dapat terjadi dalam proses bisnis tersebut.

Pada buku CISA *Review* (2008), dijelaskan bahwa pendekatan berdasarkan aset, terdapat kriteria penilaian aset-aset organsisasi, yaitu kriteria kerahasiaan aset (*confidentiality*), keutuhan aset (*integrity*), dan ketersediaan aset (*availability*), dengan penjelasan sebagai berikut:

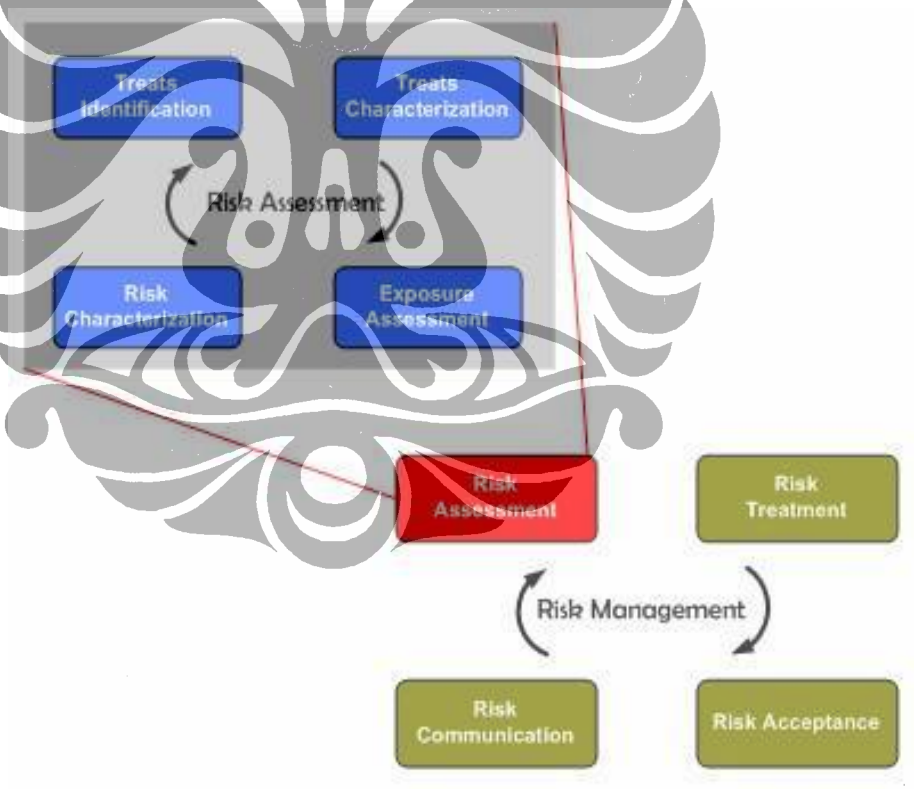
- *Kerahasiaan aset (confidentiality)*, yaitu seberapa besar kerugian yang ditimbulkan apabila terjadi hilangnya kerahasian atas suatu informasi.
- Keutuhan aset (*integrity*), yaitu seberapa besar dampak/kerugian terhadap jalannya proses bisnis, apabila suatu aset tidak digunakan dengan benar, tidak lengkap, dan tidak akurat.
- Ketersediaan aset (*availability*), yaitu seberapa besar dampak/kerugian yang ditimbulkan apabila terjadi ketidak tersediaan suatu aset.

Berdasarkan penjelasan diatas, maka pengelolaan risiko akan diawali dengan proses penilaian risiko, yang memberikan informasi tentang ancaman, kerawanan dan tingkat risiko, yang harus diwaspadai oleh perusahaan. Penjelasan mengenai penilaian risiko, akan dibahas pada bagian selanjutnya.

2.3 Penilaian Risiko (*Risk Assessment*)

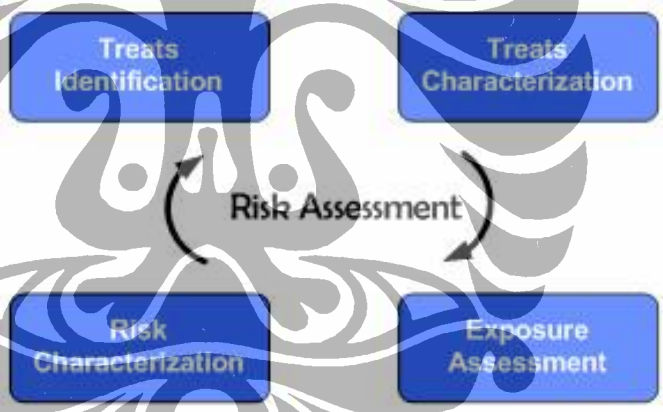
Stonebumer (2006) menjelaskan pengertian penilaian risiko (*risk assessment*) ialah proses awal pada tahapan pengelolaan risiko (*risk management*), dimana proses tersebut dilakukan untuk mengetahui secara umum tentang potensial ancaman dan risiko terkait dengan teknologi informasi yang berjalan, sehingga kemudian dapat melakukan upaya meredakan risiko (*risk mitigation*) untuk mengurangi dan menghilangkan risiko selama proses meredakan risiko.

Enisa (2006) menjelaskan bahwa pada pengelolaan risiko, dapat pula diuraikan menjadi fase-fase seperti di bawah ini, meliputi penilaian risiko (*risk assessment*), tindakan terhadap risiko (risk *treatment),* mengkomunikasikan mengenai risiko dan risiko yang harus dterima (*risk communication* dan *risk acceptance).*



Gambar 2.4 Fase pada *Risk Management* dan *Risk Assessment*

Enisa (2006) menjelaskan pula bahwa *risk assessment* merupakan upaya untuk menemukan dan mengevaluasi risiko yang berpotensi dapat mengganggu jalannya bisnis. *Risk assessment* kemudian dilanjutkan dengan *risk treatment*. *Risk treatment* merupakan kegiatan untuk memilih dan mengimplementasikan sistem kontrol keamanan untuk mengurangi risiko tersebut. *Risk treatment* juga dilakukan upaya untuk meredakan risiko (*risk mitigation*). Setelah dilakukan *risk treatment*, maka akan dilanjutkan dengan proses *risk acceptance*. *Risk acceptance* merupakan kegiatan untuk untuk melihat lebih jauh dampak atau risiko yang mungkin akan ditimbulkan dari sistem kontrol keamaan yang telah diimplementaskan. Dan kemudian *risk communication*, yaitu kegiatan untuk menginformasikan mengenai risiko dan pentingnya memperhatikannya, kepada para stakeholder dan internal perusahaan, agar timbul kesadaran untuk selalu disiplin dalam melakukan prosedur kerja yang efektif dan aman.



Gambar 2.5 Fase pada *IT Risk Assessment*

Enisa (2006) menjelaskan *IT Risk Assessment* dapat dipahami sebagai upaya untuk menilai dan menguji risiko yang mungkin dapat terjadi pada perangkat sistem dan infrastruktur yang ada *(current risk*). Fase pada *IT risk assessment*, meliputi kegiatan mengidentifikasi ancaman (*threats identification*), melakukan karakterisasi ancaman (*threat characterization*) yang berisi tentang dampak *(impact*) dan kecenderungan terkait dengan ancaman.

Selanjtnya melakukan *exposure assessment*, dengan mengidentifikasi kelemahan/kerawanan (*likelihood*). Selanjutnya melakukan *risk characterization*, yaitu mengenal tingkat risiko dan evaluasi dampaknya terhadap bisnis.

Stonebumer (2006) menjelaskan bahwa penaksiran risiko merupakan langkah-langkah yang perlu dilakukan dalam rangka untuk mengetahui tingkat risiko yang terhadap aset yang dimiliki oleh perusahaan, karena dari hal itu akan ditentukan rancangan untuk mengurangi resiko terhadap kehilangan atau kerusakan aset. Secara lengkap, 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. Rekomendasi kontrol (*control recommendation)*
9. Dokumentasi (*result documentation)*

Risiko merupakan hal yang memungkinkan akan menyebabkan ancaman terhadap aset perusahaan, yang berpotensi mendatangkan kerawanan/kelemahan (*vulnerability)* dan berdampak pada perusahaan. Untuk mengetahui kemungkinan terganggunya keamanan aset perusahaan, maka perlu dilakukan analisis dari ancaman terhadap sistem TI, dengan cara mengukur potensi kerawanan/kelemahan (*vulnerability)* dan kontrol pada sistem TI, sehingga akan disusun laporan hasil penaksiran risiko.

Dalam melakukan identifikasi risiko, terdapat dua pendekatan,

- Pendekatan *top-down*, yaitu pendekatan ini merupakan pendekatan yang dilakukan dalam mengidentifikasi risiko, yang berawal dari identifikasi risiko pada level strategis yang kemudian dapat mengarah pada level managerial yang mengidentifikasi risiko di unit-unit usaha, dan kemudian pada level operational, yang dapt berisiko terhadap aktivitas-aktivitas yang dilakukan.

- Pendekatan *bottom-up*, yaitu pendekatan risiko ini merupakan pendekatan yang dilakukan dalam mengidentifikasi risiko, yang berawal dari level operasional, yang selanjutnya di kumpulkan, sehingga dapat mengidentifikasi risiko di level manajerial, serta risiko di level strategik.

Berdasarkan penjelasan mengenai proses penilaian risiko, selanjutnya dalam beberapa literatur, dijelaskan bahwa penilaian risiko sering dikaitkan dan dikatakan memiliki sinonim kata yaitu analisis risiko (*risk analysis*), yang merupakan proses mengindentifikasi resiko keamanan dan menetapkan strategi untuk meredam risiko tersebut. Penjelasan tentang analisis risiko, akan diuraikan pada bagian selanjutnya.

2.3.1 Analisis Risiko

Krutz (2003) dalam buku berjudul "*CISSP Preparation Guide"*, menjelaskan bahwa pengertian analisis risiko ialah proses untuk mengidentifikasi risiko keamanan, menetapkan strategi untuk meredam resiko tersebut, dan identifikasi area yang membutuhkan pengamanan. Analisis risiko merupakan bagian dari *risk management*. Krutz (2003) juga menjelaskan sinonim kata dari analisis risiko adalah penilaian risiko (*risk assessment*).

Bracknel forest partnership (2008) dalam dokumen berjudul "*Startegic Risk Management Report*", menjelaskan proses analisis risiko, ialah sebagai berikut:

a. Pencatatan risiko *(risk register)*
b. Penaksiran/penilaian risiko *(risk assessment)*
c. Potensi risiko
d. Analisis risiko *(risk analysis)*
e. Profil risiko *(risk profile)*
f. Peluang *(opportunity)*

Di bawah ini adalah penjelasan dari proses analisis risiko diatas,:

- Pencatatan risiko *(risk register)*, yaitu melakukan deskripsi dari risiko, penyebab, dampak dan konsekuensi dari risiko tersebut. Hasil dari tahapan ini adalah pengidentifikasian risiko (nama risiko, deskripsi, penyebab (*cases*), dampak, dan kontrol), area risiko (area, sub-area dan risiko).
- Penaksiran/penilaian risiko *(risk assessment)*, yaitu melakukan penaksiran risiko, sehingga akan diketahui level dari risiko, yang ada, dan harus dikurangi, sehingga akan menghasilkan risiko yang tersisa.
- Potensi risiko, yaitu melakukan review secara periodik terhadap potensi risiko tersebut.
- Analisis risiko *(risk analysis),* yaitu melakukan analisis terhadap risiko yang berhasil di register diawal proses. Terdapat tiga pendekatan dalam analisis risiko, yaitu:
  - Metode analisis kualitatif *(qualitative analysis method)*, yaitu metode analisis risiko yang menggunakan tabulasi berdasarkan penilaian deskriptif (tinggi, sedang atau rendah).
  - Metode analisis kuantitatif *(quantitative analysis method)*, yaitu metode analisis risiko yang menggunakan angka numerik untuk menyatakan dampak dan probabilitas.
  - Metode analisis semi kuantitatif, yaitu metode analisis risiko yang menggunakan angka skala untuk tiap kategori kualitatif.
- Profil risiko *(risk profiles)*, yaitu menampilkan tingkatan risiko, dalam bentuk koordinat kecenderungan (*likelihood*) dan dampak (*impact*).
- Peluang (*opportunity*), yaitu dalam proses pengelolaan risiko, terdapat peluang untuk melakukan *improve* dan pemeliharaan aset terhadap ancaman risiko.

Pada analisis risiko kuantitatif dan kualitatif, masing-masing memiliki tahapan. Secara umum tentang metode analisis risiko secara kuantitatif dan kualitatif, akan dijelaskan pada bagian selanjutnya.

2.3.2 Analisis Risiko Kuantitatif

Metode analisis kuantitatif *(quantitative analysis method)*, yaitu metode analisis risiko yang menggunakan angka numerik untuk menyatakan dampak dan probabilitas. Pada dokumen *information assurance* CS498SH (2006), menjelaskan bahwa pada pendekatan kuantitatif, dilakukan dengan enam proses penting, meliputi:

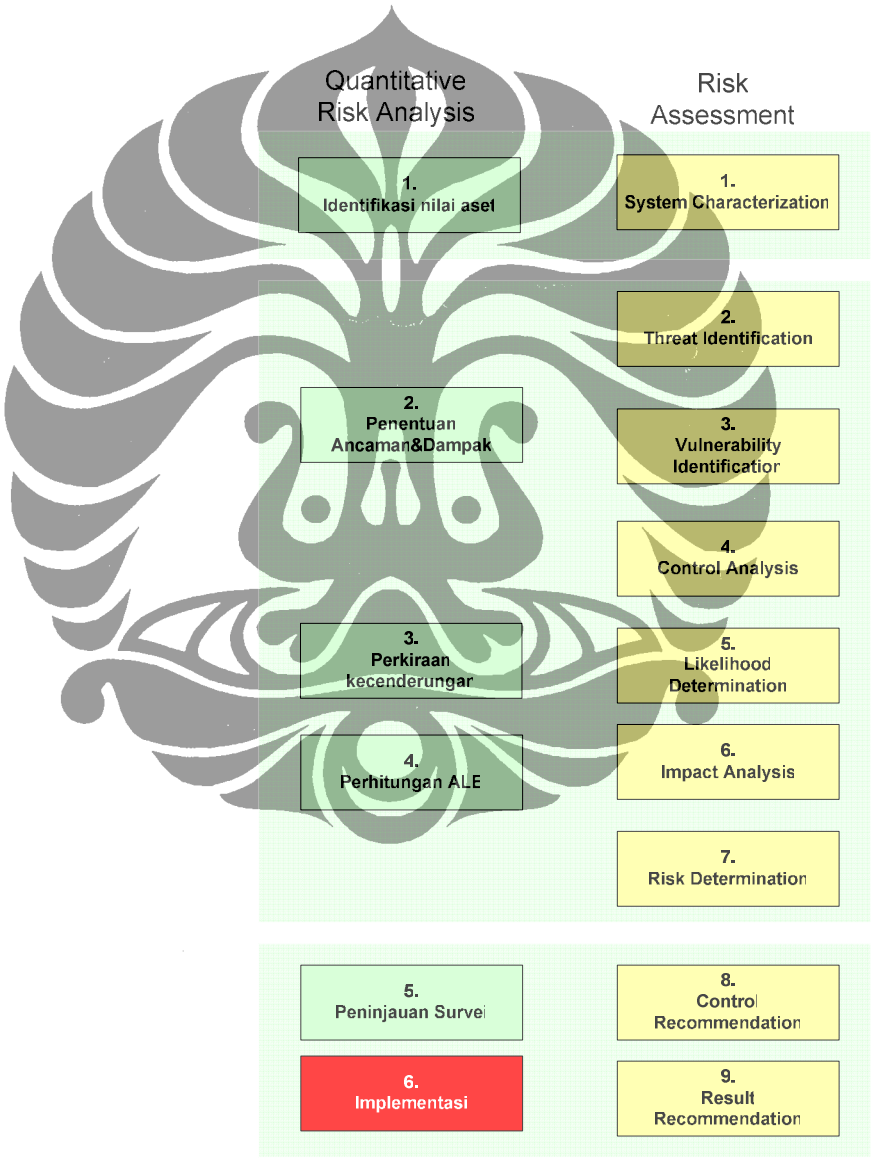
a. Identifikasi nilai aset (*asset value*)
b. Penentuan ancaman, kelemahan (*vulnerability*) dan dampak
c. Perkiraan kecenderungan terjadi (*likelihood of exploitation*).
d. Perhitungan *Annual Loss Exposure* (ALE)
e. Peninjauan (*survey*) penggunaan kontrol dan biayanya
f. Pelaksanaan project untuk implementasi kontrol

Berikut ini adalah penjelasan dari enam proses pada analisis risiko dengan pendekatan kuantitatif:

- Identifikasi nilai aset: ialah nilai moneter yang dimiliki aset, berdasarkan actual cost, atau biaya pengganti dari aset tersebut. (*asset value*).
- Penentuan ancaman, kelemahan dan dampak: ialah mengetahui frekuensi ancaman (*threat frequency*) yang pernah terjadi, analisis terhadap kelemahan (*vulnerability analysis*), dan perhitungan dampak (*impact analysis*).
    - *Threat Frequency* (ARO): mengetahui seberapa sering ancaman terjadi, yang disebut dengan *Annual Rate Occurance* (ARO), contoh: kebakaran besar 1 dalam 40 tahun, system crash 1 dalam 6 bulan.
    - *Vulnerability Analysis* (EF): mengetahui pontensi kehilangan aset, yang disebut Exposure factor (EF), yang merupakan presentase kehilangan akibat ancaman yang terjadi terhadap aset.
    - *Impact Analysis* (SLE dan ALE): melakukan perhitungan terhadap dampak dari kejadian gangguan keamanan, yang terkait dengan *Single Loss Expectancy* (SLE), yaitu nilai moneter yang akan hilang pada satu kali kejadian gangguan keamaan informasi.

- Perhitungan *Annual Loss Exposure* (ALE), yaitu nilai moneter yang akan hilang karena gangguan keamanan terhadap aset, pada jangka waktu satu tahun.

Berdasarkan uraian diatas, dapat dijelaskan bahwa tahapan pada analisis risiko secara kuantitatif, secara umum memiliki kesamaan dengan langkah-langkah yang ada pada penilaian risiko (*risk assessment*), sehingga dapat digambarkan sebagai berikut:



Gambar 2.6 Analisis Risiko Kuantitatif dan Penilaian Risiko

Tahapan yang ada pada analisis risiko kuantitatif, memiliki fungsi yang sama dengan tahapan yang ada pada penilaian risiko. Contohnya identifikasi nilai aset, dapat dilihat sebagai proses untuk mengidentifikasi karakteristik sistem seperti teknologi, informasi dan manusia. Tetapi tahap implementasi dari kontrol yang terdapat pada analisis risiko kuantitatif, tidak dimiliki pada penilaian risiko, karena penilaian risiko hanya sampai pada usulan kontrol, berdasarkan penilaian risiko yang dilakukan.

2.3.3 Analisis Risiko Kualitatif

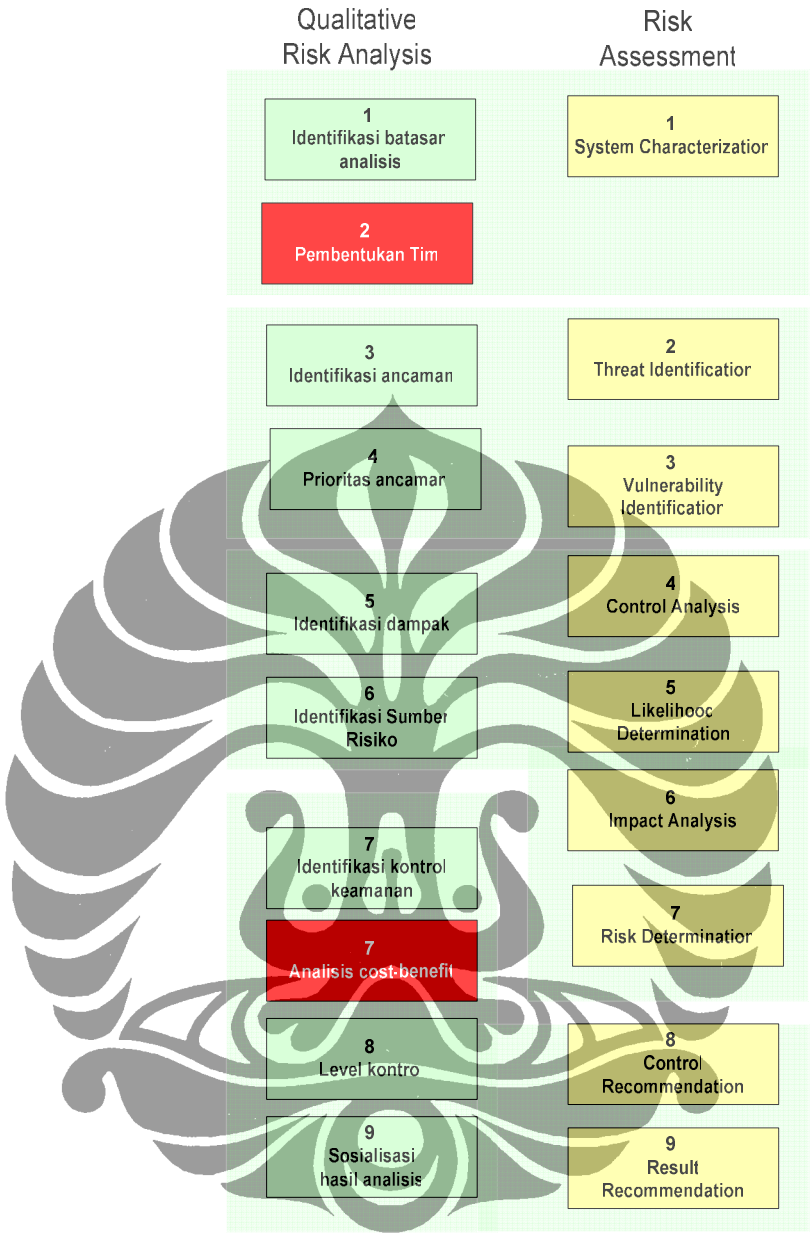
Metode analisis kualitatif *(qualitative analysis method*), yaitu metode analisis risiko yang menggunakan tabulasi berdasarkan penilaian deskriptif (tinggi, sedang atau rendah). Pendekatan kualitatif melakukan analisis terhadap potensi dampak yang dapat terjadi akibat ancaman dari gangguan dan kelemahan, yang akan dinilai dengan skala tinggi, menengah dan rendah.

Peltier (2001), dalam bukunya yang berjudul "*Information Security Risk Anaysis*", menjelaskan tahapan pada analisis risiko secara kualitatif, dalam sepuluh proses, meliputi:

a. Identifikasi batasan analisis (*scope*)
b. Pembentukan tim.
c. Identifikasi ancaman
d. Prioritas ancaman berdasarkan aset
e. Dampak kehilangan
f. Rekapitulasi ancaman, dampak dan risiko
g. Identifikasi kontrol dan pengamanan
h. Analisis cost-benefit
i. Level kontrol
j. Sosialisasi hasil analisis

Penjelasan dari sepulug proses analisis risiko kualitatif, sebagai berikut:

- Identifikasi batasan analisis: proses ini akan dilakukan penentuan fokus masalah yang akan diselesaikan.
- Pembentukan tim: pada proses ini akan dilakukan pembentukan tim yang bisa terdiri dari para ahli, pihak managemen dan pengguna.
- Identifikasi ancaman: pada proses ini akan dilakukan pendaftaran beberapa ancaman, berdasarkan hasil observasi dan tanya jawab, sehingga dapat diketahui ancaman dan kelemahan yang menyebabkannya.
- Prioritas ancaman berdasarkan aset: pada proses ini memperhatikan ancaman yang memiliki kecenderungan terjadi dinilai rendah, menengah atau tinggi.
- Dampak kehilangan: berdasarkan identifikasi dampak kehilangan, maka dapat dinilai level dampaknya, yang dinilai dengan rendah, menengah dan tinggi.
- Rekapitulasi ancaman, dampak dan risiko: pada proses ini akan dilakukan rekapitulasi level ancaman, dampak dan faktor risiko.
- Identifikasi kontrol/pengamanan: pada proses ini akan dilakukan identifikasi kontrol dan alat pengamanan yang akan dipilih berdasarkan ancaman.
- Sosialisasi hasil analisis: melakukan pembuatan *executive summary*, yang melaporkan keseluruhan hasil analisis risiko yang dilakukan.



Gambar 2.7 Analisis Risiko Kualitatif dan Penilaian Risiko

Proses pada analisis risiko kualitatif memiliki fungsi yang sama seperti proses pada penilaian risiko, sebagai contoh penilaian dampak kehilangan yang dilakukan pada analisis risiko kualitatif, sama dengan tahap analisis dampak pada penilain risiko, tetapi tahap analisis *cost-benefit* tidak terdapat pada penilaian risiko, karena analisis tersebut ada pada tahapan *risk mitigation*.

Berdasarkan kajian teori analisis kualitatif dan kuantitatf diatas, maka masing-masing dapat digunakan sebagai dukungan dalam melakukan penilaian risiko, selanjutnya akan dijelaskan tentang perbandingan analisis kuantitatif dan kualitatif itu sendiri, agar memiliki dasar dalam menggunakan kedua metode analisis diatas, sebagai pendukung dalam melakukan penilaian risiko.

2.3.4 Analisis Risiko Kuantitatif dan Kualitatif

Romania dan Adrian (2005) ini menemukan terdapat keterbatasan pada kedua metode analisis risiko kuantitatif dan kualitatif. Hal tersebut diperoleh setelah melakukan perbandingan berdasarkan dua faktor, yang merupakan dampak dari *risk assessment*, yaitu *time constraint* dan *moral hazard*. Manager IT mengetahui bahwa dalam keamanan jangka panjang sistem informasi (SI) adalah hal ideal yang ingin dicapai, dan pengaruh finansial dari lemahnya kebijakan, prosedur, dan standar keamanan informasi, merupakan hal yang sulit untuk diukur atau dinilai, sehingga perhitungan tersebut menjadi kurang akurat.

Romania dan Adrian (2005) menyimpulkan bahwa pengukuran resiko keamanan merupakan pekerjaan yang sulit, yang hampir tidak mungkin dilakukan secara akurat, untuk sebuah SI. Pada literatur keamanan informasi, dapat dilihat bahwa dalam metode kuantitatif terdapat tahapan penilaian *value of the assets*. Dalam memperoleh nilai aset, seperti aset berupa informasi atau database, sangat terbuka peluang munculnya subjektifitas penilai. Sebab dalam penilaian tersebut, terdiri dari beberapa elemen yang harus ditaksir. Elemen tersebut antara lain, nilai dari kompetitis aset, biaya perangkat lunak, biaya untuk melindunginya, dan lain-lain. Sedangkan pada metode kualitatif menggunakan kuesioner untuk memperoleh fakta, melalui estimasi secara statistik, dengan penilaian *low, medium* dan *high*, sehingga ditemukan kesulitan dalam menghitung kerugian finansial jika hanya berdasarkan asumsi atau judgment.

Romania dan Adrian (2005) menyimpulkan bahwa kedua pendekaan diatas dalam proses analisisnya sangat dipengarui oleh subjektifitas penilainya, sehingga pengguna metode tersebut, harus menggunakan kedua-dua secara satu kesatuan dan seimbang, untuk memperoleh hasil yang lebih sempurna.

Valentin (2007) menyatakan bahwa penilaian resiko dilakukan untuk mengurangi kerugian, tetapi dalam operasionalnya masih ditemukan pertanyaan, apakah harus memilih salah satu pendekatan, antara pendekatan kualitatif atau kuantitatif.

Valentin (2007) menyimpulkan bahwa pada pendekatan kualitatif sangat didominasi oleh pengukuran yang subjektif, sedangkan pada pendekatan kuantitatif dapat meniadakan sifat subjektif yang ada, sehingga akan lebih objektif dibandingkan metode kualitatif.

Menurut Romania&Adrian (2005) pada artikel pertama dan Valentin (2007) pada artikel yang kedua, *risk assessment* menggunakan pendekatan kualitatif menggunakan skala *high-medium-low* dalam menangkap fakta berdasarkan elemen-elemen *risk assessment*. Sedangkan pada pendekatan kuantitatif, digunakan angka-angka yang terukur, untuk menilai elemen-elemen *risk assessment*. Berdasarkan komparasi diatas, maka kedua artikel ini memiliki kesamaan dalam melihat kedua pendekatan tersebut

Hasil penelitian yang dituliskan oleh Romania&Adrian (2005), bahwa pendekatan kualitatif dan kuantitatif, sama-sama tidak dapat terlepas dari penilaian yang bersifat subjektif, karena pada pendekatan kuantitatif pun ditemukan tahapan dimana perlu dilakukan sebuah perkiraan dan judgment dari peneliti agar dapat menilai *value of asset*, nilai dari kompetitif aset, biaya perangkat lunak, biaya untuk melindunginya. Sedangkan hasil penelitian yang ditulsikan oleh Valentin (2007), menyatakan bahwa pendekatan quantitif dapat menghilangkan penilaian yang bersifat subjektif, karena melakukan penilaian dengan angka-angka yang akurat dan terukur.

Romania dan Adrian (2005) mencoba menguraikan langkah-langkah pendekatan kuantitatif, sehingga menemukan tahapan penilaian yang tidak dapat lepas dari subjektifitas penggunanya. Sedangkan Valentin (2007), hanya melihat aspek yang memang dapat dinilai dengan angka dan rumus yang jelas, contoh nya EF, ARO, atau ALE, sedangkan aspek dalam penentuan nilai aset tidak dijelaskan bahwa terdapat faktor yang mungkin tidak dapat dilakukan dengan objektif, karena dipengaruhi oleh subjektifitas atau judgment penilainya, contohnya nilai kompetitif dari aset, yang tidak dapat diukur secara akurat. Hal ini menyebabkan kesimpulan yang berbeda antara penelitian di artikel pertama dan kedua.

Romania dan Adrian (2005) menjelaskan bahwa baik pendekatan kualitatif atau kuantitatif pada risk assessment, tidak dapat terlepas dari subjektifitas penilainya, sedangkan Valentin (2007) menyatakan bahwa pendekatan kuantitatif akan menghilangkan sifat penilaian yang subjektif, sehingga perlu menggunakan kedua metode ini secara seimbang, agar dapat diperoleh hasil penilaian yang seimbang dan objektif.

Romania&Adrian (2005) dan Valentin (2007) memberikan rekomendasi pendekatan terbaik dalam melakukan *risk assessment*, agar hasil penilaian dapat bersifat objektif dan seimbang, yaitu dengan cara menggunakan kedua pendekatan tersebut (kuantitatif dan kualitatif) atau semi-kuantitatif, agar keterbatasan dari setiap pendekatan dapat diperbaiki, dan yang paling penting adalah dalam penilaian sedapat mungkin mengurangi subjektifitas, agar hasil risk assessment dapat dijadikan dasar yang kuat, dalam membuat strategi penanganan resiko.

2.4 Mitigasi Risiko (Risk Mitigation)

Stonebumer (2006) menjelaskan bahwa pada tahap penilaian risiko, telah diperoleh tingkat risiko yang berpotensi dihadapi. Selanjutnya harus dilakukan *risk mitigation,* yang bertujuan untuk melakukan tindakan proaktif untuk menurunkan dan mencegah risiko tersebut terjadi dan menganggu jalannya bisnis.

Pada panduan yang dikeluarkan oleh SOMAP.org yang berjudul *"Open Information Security Risk Management Handbook"* (2006), *Risk mitigation* dilakukan tidak hanya untuk menurunkan risiko, tetapi juga mengurangi dampak negatif terhadap keberlanjutan bisnis. Pilihan strategi yang akan tentukan pada tahap *risk mitigation*, sebagai berikut:

- Penghilangan risiko (*risk elimination/avoidance*) ialah upaya untuk menentukan aksi, yang bertujuan menghilangkan risiko tertentu terjadi. Sebagai contoh jika perusahaan belum menentukan rancangan darurat, jika terjadi bencana pada sistem TI perusahaan, hal ini akan sangat berdampak pada jalannya bisnis perusahaan, sehingga langkah risk mitigation ialah dengan menyusun dan menetapkan kebijakan perusahaan tentang DRP (*disaster recovery plan*) dan BCP (*business continuity plan*).
- Pengurangan risiko *(risk reduction)* ialah upaya untuk mengurangi dampak, yang dapat menyebabkan terganggunya keberlangsungan bisnis. Sebagai contoh pada proses backup yang rutin dilakukan, menghasilkan file backup, tetapi belum ada jaminan bahwa file backup tersebut pasti berhasil di-restore dengan baik. Hal ini berpotensi kemungkinan gagalnya file yang direstore, sehingga langkah risk mitigation ialah perlu dilakukan uji coba secara rutin terhadap file backup tersebut, untuk mengurangi risiko file backup yang gagal digunakan.
- Pemindahan risiko *(risk transfer)* ialah upaya untuk mengirim risiko ke tempat lain. Sebagai contoh perusahaan mengasuransikan peluang kerugian yang mungkin dapat dialami oleh perusahaan, jika terjadi gangguan keamanan pada sistem TI.

- Penerimaan risiko (*risk acceptance*) ialah sikap untuk menerupa risiko, terutama residual risk, yang tersisa setelah dilakukan penanggulangan risiko.

Risk mitigation merupakan tahapan lanjutan pada proses pengelolaan risiko setelah melakukan penilaian risiko, dimana dalam *risk mitigation* terdapat penentuan prioritas, evaluasi, implementasi dan pemeliharaan upaya menanggulangan dampak dari risiko, berdasarkan identifikasi yang dilakukan pada tahap penaksiran risiko. Untuk menghilangkan secara keseluruhan risiko, pada prakteknya sangat tidak mungkin, kerena itu merupakan tanggungjawab manajemen untuk melakukan pendekatan dalam upaya menurunkan tingkat risiko.

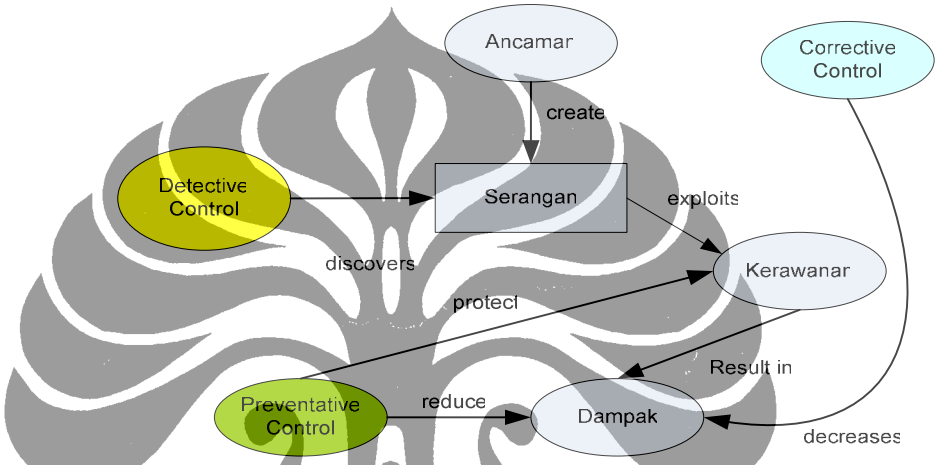
Risk mitigation akan mengarahkan pimpinan untuk menyeimbangkan opersional dan biaya ekonomi yang harus dikeluarkan sebagai upaya proaktif dalam melindungi aset yang dimiliki, karena akan dilakukan evaluasi terhadap kontrol keamanan informasi, yang dibutuhkan dalam upaya mitigasi risiko.

Kontrol keamanan informasi yang bersifat internal ialah kebijakan, prosedur, kebiasaan dan struktur organisasi yang dirancang untuk menjamin keamanan informasi, dan mampu melakukan pencegahan, pendeteksian dan koreksi. Sedangkan kontrol keamanan yang bersifat eksternal ialah perangkat berupa hardware dan software yang diperoleh dari luar organisasi, dan diimplementasikan di sistem TI organisasi tersebut.

Menurut Ronald di Buku CISSP *Guide*, dengan menggunakan kontrol keamanan informasi, diharapkan akan mampu meredam risiko yang ada, dimana kontrol akan memiliki fungsi sebagai berikut:

- Kontrol pencegahan *(preventive control)*, yaitu kontrol yang befungsi melakukan pencegahan dari upaya-upaya melanggar kebijakan dan aturan keamanan informasi.

- Kontrol pendetaksi *(detective control)*: yaitu kontrol yang berfungsi melakukan peringatan adanya pelanggaran yang terjadi sebagai upaya pelanggaran kebijakan atau aturan keamanan informasi. Beberapa detective control overlap dengan preventive control, karena sebuah kontrol dapat digunakan sebagai preventive untuk masa depan, dan detective untuk kejadian saat ini.
- Kontrol koreksi *(corrective control),* yaitu kontrol yang berfungsi untuk melakukan recovery dari dampak yang telah ditimbulkan oleh terjadinya risiko.



Gambar 2.8 Penanganan Serangan

Sebuah serangan yang terjadi, karena adanya potensi ancaman, yang dapat dihidari menggunakan *defferent control*. Serangan dapat dikenali dengan menggunakan *detective control*, dan serangan terjadi karena adanya kerawanan/kelemahan, yang berdampak negatif bagi organisasi. Dampak dan kerawanan/kelemahan tersebut dapat dihindari dengan adanya *preventive control*, dan diperbaiki dengan *corrective control*.

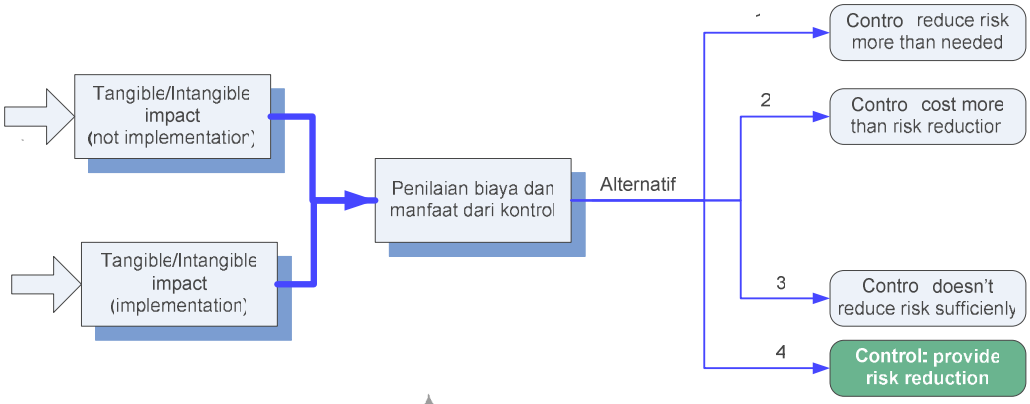
Selanjutnya kontrol keamanan informasi yang diusulkan, sebagai upaya untuk melakukan mitigasi terhadap risiko, harus dianalisis sisi manfaatnya dengan melakukan *cost-benefit analysis*, sehingga diperoleh perbandingan nilai manfaat yang akan diberikan, dengan melihat biaya atau dampak yang diterima jika diimplemetasikan atau tidak diimplementasikan kontrol keamanan tersebut bagi perusahaan

2.4.1 Cost-Benefit Analysis

Dalam melakukan alokasi dan implementasi *cost-effectiveness*, sebelumnya organisasi perlu melakukan analisis *cost-benefit*, yang bertujuan untuk menilai manfaat yang akan diberikan, dengan melihat biaya atau dampak yang diterima jika diimplemetasikan atau tidak diimplementasikan kontrol keamanan tersebut bagi perusahaan

Menurut Stoneburner (2002) dalam dokumen standar NIST (*National Institute of Standards and Technology*), bahwa analisis *cost-benefit* dapat dilakukan secara kualitatif atau kuantitatif. Analisis ini bertujuan untuk menunjukkan bahwa biaya dan dampak implementasi kontrol dapat secara sesuai mengurangi risiko, contohnya organisasi harus menolak mengeluarkan biaya Rp.5.000.000,- untuk kontrol yang hanya mampu mengurangi risiko kerugian sekitar Rp.1.000.000, atau dengan kata lain dampak yang diterima jika diimplementasikan, tidak lebih besar dengan dampak jika tidak diimplementasikan.

Analisis *cost-benefit* dilakukan dengan beberapa tahapan, meliputi (1)mengidentifikasi dampak, jika kontrol tertentu diiimplementasi (*tangible and intangible)*; (2)mengidentifikasi dampak, jika tidak mengimpelemtasikan kontrol tersebut (*tangible and intangible*). Biaya implementasi biasanya terkait dengan biaya pembelian perangkat keras dan software, biaya pembuatan kebijakan dan prosedur, biaya peningkatan fungsional kontrol keamanan informasi, biaya perekrutan penambahan personil, biaya trainning dan maintenance.



Gambar 2.9 Skema Tahapan Analisis Cost Benefit

Berdasarkan tahapan diatas, maka proses pada analisis *cost-benefit*, akan menghasilkan sebuah rekomendasi untuk setiap usulan kontrol, yaitu

- Jika kontrol dapat mengurangi nilai risiko lebih dari yang dibutuhkan, maka perlu dipertimbangkan biaya implementasinya yang lebih murah dan dapat mengurangi risiko minimum risiko.
- Jika kontrol akan membutuhkan biaya pembangunan pengurangan risikonya lebih besar dibanding biaya risikonya, maka perlu mencari alternatif kontrol lain.
- Jika kontrol kontrol tidak dapat mengurangi minimal risiko, maka perlu mencari alternatif lain.
- Jika kontrol mengurangi minimum resiko dengan biaya implementasi yang lebih kecil dibanding biaya (nilai risiko) jika tidak diimplementasi, dan *cost effectiveness*, maka kontrol ini layak dipilih untuk diimplementasikan.

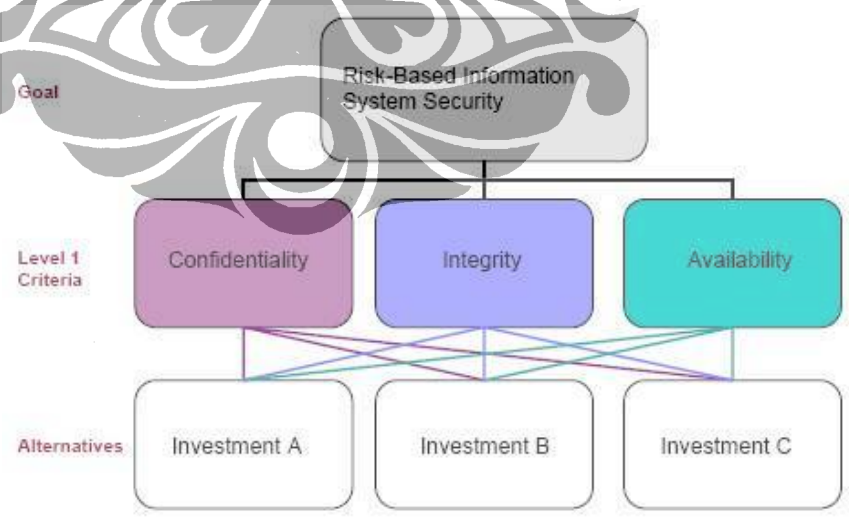
Hasil penilaian diatas, adalah hasil dari proses analisis *cost-benefit* untuk setiap kontrol yang direkomendasikan, sehingga akan ditentukan tingkat kelayakan sebuah kontrol untuk diimplementasikan. Hasil dari analisis ini, kemudikan harus didukung oleh analisis *cost-effectiveness*, yang akan memberikan penilaian terhadap kontrol-kontrol, sehiingga akan diperoleh urutan prioritas implementasi, sehingga dapat secara efektif mencapai tujuan keamanan informasi.

2.4.2 Cost-Effectiveness Analysis

Analytic Hirarchy Process (AHP) dibangun oleh. Saaty pada tahun 1970. AHP menjelaskan tentang tahapan pada *cost-effectiveness* pada ASTM Standard E 1765-02, "*Standard Practice for Applaying Analytic Hierarchy Process (AHP) to Multiattribute Decision Analtsis of Investments Related to Building and Building System*".

Menurut Barbara C. Lippiatt (2007), AHP memiliki 3 langkah utama, yaitu (1)melakukan dekomposisi kompleksitas masalah ke dalam klasifikasi dalam sebuah hirarki, dengan mengidentifikasi rancangan investasi. (2)melakukan perbandingan antar investasi berdasarkan keterkaitan dan dukungannya, dengan cara melakukan perhitungan nilai prioritas. (3) melakukan perhitungan yang menjadi agregasi dari pengukuran sebelumnya, sehingga diperoleh ranking prioritas.

Pada tahap pertama, dilakukan dekomposisi faktor-faktor dari kompleknya masalah dalam pengambilan keputusan. Di bawah ini adalah salah satu contoh hirarki yang akan menunjukkan investasi yang akan dilakukan dengan menunjukkan hubungannya dengan kriteria yang ada, dengan mengidentifikasi rancangan investasi.



Gambar 2.10 AHP Hierarchy

Pada gambar diatas, dijelaskan bahwa terdapat beberapa alternatif investasi terkait dengan implementasi kontrol keamanan informasi. Dari beberapa investasi diatas, dikaitkan dengan criteria keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan data (*integrity*), ketersediaan data (*availability*).

Tahap kedua ialah melakukan perbandingan investasi satu dengan investasi lainnya. Dalam contoh diatas, misalnya akan dibandingkan investasi A dengan investasi B dan C. Dalam perbandingan tersebut terdapat nilai yang menjadi hasil dari perbandingan tersebut. Nilai pebandingan tersebut, seperti rancangan ini:

Tabel 2.1 Skala Nilai Perbandingan (NIST Standard)

Intensity of Importance	Definition	Explanation
1	Equal importance of elements	Two elements contribute equally to the higher-level element
3	Moderate importance of one element over another	Experience and judgment slightly favor one element over another
5	Strong importance of one element over another	Experience and judgment strongly favor one element over another
7	Very strong importance of one element over another	An element is strongly favored and its dominance is demonstrated in practice
9	Extreme importance of one element over another	The evidence favoring one element over another is of the highest possible order of affirmation
2, 4, 6, & 8	Intermediate values between two adjacent judgments	Used when compromise is needed between two judgments
Reciprocals	If element i has one of the above numbers assigned to it when compared with element j, then j has the reciprocal value when compared with i.	

Dalam melakukan perbandingan elemen dalam hirarki AHP, akan dilakukan penentuan tingkat kepentingan suatu elemen dibanding elemen yang lain. Nilai perbandingan juga dapat berbentuk nilai real, contohnya 1/3. Jika nilai 3 berarti pengambil keputusan menilai bahwa investasi A ialah '*moderately more important'* dibanding investasi B. Jika ternyata pengambil keputusan, menilai bahwa terjadi sebaliknya, yaitu investasi B yang dinyatakan 'moderately more important' dibanding investasi A, maka hasil perbandingan investasi A terhadap B ialah 1/3.

Tahap ketiga ialah '*Aggregation of Relative Weight and Rating'*, yaitu melakukan penggabungan hasil penilaian tersebut dalam sebuah tabel perhitungan, sehingga akan menemukan nilai prioritas dari setiap alternatif investasi.

Analisis *cost-effectiveness* akan memberikan urutan prioritas kontrol keamanan informasi yang akan diimplementasi, berdasarkan kemampuannya dalam mencapai tujuan keamanan informasi yang diharapkan. Berdasarkan hasil analisis *cost-effectiveness* dan *cost-benefit*, maka akan dibuat sebuah rancangan keamanan informasi. Penjelasan tentang perancangan keamanan informasi, akan dibahas pada bagian selanjutnya.

2.4.3 Kebijakan Keamanan Informasi

Danchev (2003) menjelaskan bahwa kebijakan keamanan informasi merupakan bagian penting dari keamanan informasi. Sebagai contoh kebijakan penggunaan *firewall*, sebagai akses kontrol aliran informasi dari luar ke dalam. Standard, prosedur dan *guideline* yang ada di perusahaan harus merujuk pada kebijakan keamanan yang ditetapkan.

Joel Weise (2001) menjelaskan bahwa penyusunan kebijakan keamanan yang baik, ialah jika didukung oleh pemahaman yang baik tentang penanganan keamanan terhadap gangguan atau bencana berdasarkan analisis risiko yang telah dilakukan. Terdapat beberapa jenis kebijakan keamanan informasi:

- Kebijakan mengenai program *(program policy)*, yaitu kebijakan program yang mengandung lima tujuan:
  - *Avoidance*, ialah kemampuan untuk mencegah unauthorized access.
  - *Detection*, ialah kemampuan untuk mengidentifikasi penyusupan.
  - *Investigation*, ialah kemampuan untuk melakukan teknik penyelidikan untuk menemukan penyusup.
  - *Continuity*, ialah kemampuan untuk menjamin adanya rancangan penyelamatan dari bencana.

- Kebijakan klasifikasi informasi/aset *(information/resource classification)*, yaitu kebijakan untuk melakukan kategorisasi informasi yang sensitif dan kritikal, agar dapat mengetahui pengamanan terhadap informasi tersebut.
- Kebijakan standard akses *(standard access definition)*, yaitu kebijakan yang berisi tentang tiga prinsip standard access: Individual accountability, Least privilege, Separation of duties
- Kebijakan manajemen password *(password management policy)*, yaitu kebijakan yang akan memperhatikan kehandalan password yang digunakan (*length and strength checks*)
- Kebijakan penggunaan internet *(internet usage policy)*, yaitu kebijakan yang menjelaskan user dapat memiliki fasilitas koneksi internet (email, web, ftp, chat).
- Kebijakan keamanan jaringan *(network security policy)*, yaitu kebijakan untuk melindungi akses terhadap jaringan yang terhubung dengan seluruh komputer dan sumber-sumber informasi.
- Kebijakan akses *(remote access policy)*, yaitu kebijakan yang mengatur izin dilakukannya remote access.
- Kebijakan penggunaan dekstop *(dekstop policy)*, yaitu kebijakan yang mengatur tentang pemanfaatan screenserver, serta aplikasi yang berjalan di PC dekstop, seperti antivirus, file attachment)
- Kebijakan platform server *(server plarform policy)*, yaitu kebijakan yang mengatur tentang penggunaan operating system pada server yang berbeda dengan PC.
- Kebijakan keamanan aplikasi *(application security)*, yaitu kebijakan yang mengatur tentang penggunaan operating system pada server yang berbeda dengan PC.

Kebijakan keamanan informasi diatas, akan sangat penting bagi implementasi setiap kontrol, sehingga akan menajdi bagian penting dalam rekomendasi rancangan keamanan informasi. Penjelasan dalam perancangan keamanan akan dibahas pada bagian selanjutnya.

2.5 Perancangan Keamanan Informasi

Pada artikel lembaga *Information Ass Spring* (2008) dijelaskan bahwa rancangan keamanan informasi (*information security planning*) merupakan susunan strategi yang diterapkan untuk mengurangi kelemahan dan menurun potensial ancaman dan risiko terkait dengan teknologi informasi yang berjalan, sehingga kemudian dapat melakukan proses untuk meredakan risiko (*risk mitigation*), dan melakukan kontrol dan evaluasi.

Komponen dari rancangan 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 akan menjadi kebutuhan penting rancangan ini adalah permintaan akan level pengamanan yang diinginkan.

Rancangan keamanan menjadi sangat penting, karena sebagai dasar dalam mengembangan 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.

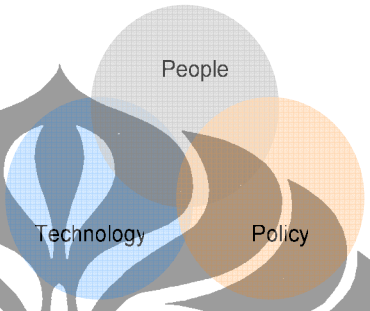
Pada dokumen *Information Security Plan Template*, yang dikelurkan oleh OTDA, keamanan informasi mengandung konsep lainnya, yaitu pengelolaan risiko, kebijakan (*policy*), prosedur (*procedure*), standar (*standards*), petunjuk (*guidelines*), klasifikasi informasi (*information clasification*), operasi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

Gambar 2.11 CIA *triangle*

Sesuai dengan gambar diatas, Muhammad Sholeh (2007) menjelaskan bahwa terdapat prinsip-prinsip penting dari sebuah rancangan keamanan informasi (*information security*), ialah 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: :

- Kerahasiaan *(confidentiality),* yaitu membatasi akses informasi hanya bagi pengguna tertentu dan mencegah orang yang tidak berhak memperoleh informasi tersebut. Implementasi konsep *confidentiality* salah satunya adalah user ID dan password dalam skema otentikasi.
- Keutuhan data/informasi *(integrity),* yaitu taraf kepercayaan terhadap sebuah informasi. Dalam konsep ini tercakup *data integrity* dan *source integrity*. Keutuhan data terwujud jika data/informasi belum diubah (masih asli), baik perubahan yang terjadi karena kesalahan atau dilakukan sengaja oleh seseorang.
- *Ketersediaan (availability),* yaitu ketersediaan, betul sekali. *Availability* yang dimaksud adalah ketersediaan sumber informasi. Jika sebuah sumber informasi tidak tersedia ketika dibutuhkan, bahkan bisa lebih buruk lagi. Ketersediaan ini bisa terpengaruh oleh faktor teknis, faktor alam maupun karena faktor manusia. Meskipun ada tiga faktor yang berpengaruh, tetapi umumnya manusia adalah link paling lemahnya. Karenanya, wajar jika Anda perlu memperhatikan perlunya menggunakan tools untuk *data security*, misalnya sistem backup atau anti virus.

Selanjutnya Amti Sodiq (2009) menjelaskan bahwa pada sebuah rancangan 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.



Gambar 2.12 ***People, policy and technology model***

Sebuah rancangan 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)*, kontrol yang dilakukan terhadap internal seperti penyusunan kebijakan, prosedur, standar, dan petunjuk, guna pengamanan informasi.
2. Kontrol logik *(logical control)*, yaitu kontrol teknikal yang dilakuakan untuk pengamanan informasi, antara lain dengan misalnya menggunakan passwords, *authentication control*, *firewalls*, *intrusion detection*, dan anti-virus.
3. Kontrol fisik *(physical control)*, yaitu kontrol secara fisik yang dilakukan untuk pengamanan informasi dari penyalahgunaan (*misuse*), pencurian (*theft*), perusakan (*vandalism*), bencana alam (*natural disasters*).

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*) .

Berdasarkan uraian diatas, maka rancangan keamanan akan berisi tentang penentuan kombinasi kontrol keamanan informasi yang digunakan, serta prioritas dalam melakukan implementasinya. Di bawah ini merupakan isi/konten dasar pada dokumen rancangan keamanan informasi (*information security plan*), antara lain:

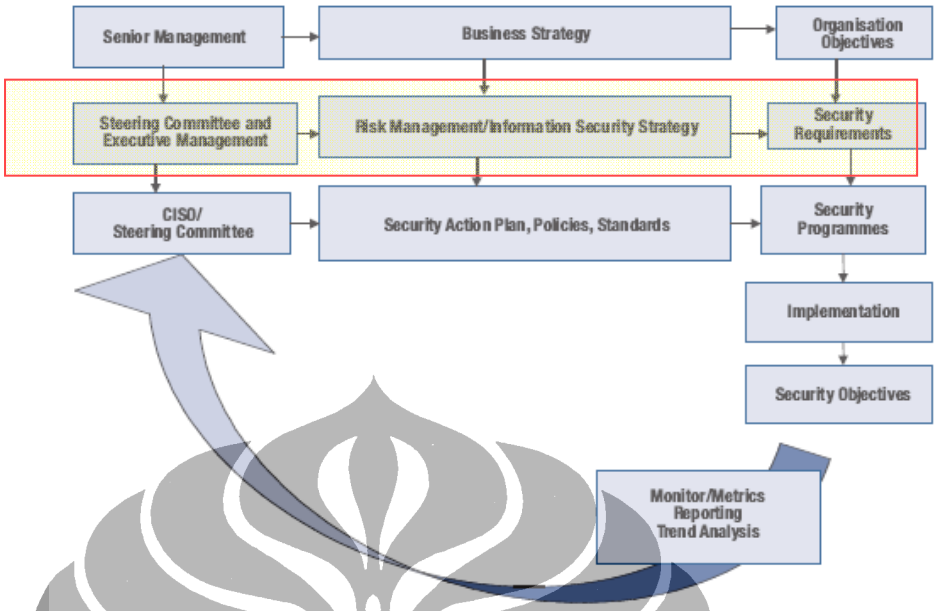
1. Ancaman dan kelemahan, merupakan proses untuk mereview hasil tahapan penilaian risiko, dengan mengambil informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi jika terjadi (ancaman), yang memanfaatkan kerawanan/kelemahan yang dimiliki oleh perusahaan.
2. Tujuan dan sasaran, merupakan 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. Aaturan dan tanggungjawab, merupakan proses menyusun aturan dan penanggungjawab, yang akan 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.

Kontrol yang telah ditentukan pada rancangan keamaanan informasi, diharapkan dapat secara efektif meredakan risiko gangguan terhadap keamanan informasi pada perusahaan. Salah satu jenis kontrol yang menentukan keberhasilan keamanan informasi pada sebuah organisasi ialah kebijakan (*policy*) tentang keamanan informasi. Penjelasan tetang kebijakan keamanan informasi, akan dibahas pada bagian selanjutnya.

2.6 Tatakelola Keamanan Informasi (*Information Security Governance*)

Pada buku yang berjudul "*Informatioan Security Governance: Guidance*" yang dikeluarkan oleh IT *Governance Institute* (IT-GI), menjelaskan tatakelola keamanan informasi mengandung konsep kepemimpinan, struktur organisasi dan proses dalam keamanan informasi. Tatakelola dijelaskan sebagai kumpulan tanggungjawab dan aturan untuk menjalankan strategi keamanan informasi, sesuai dengan tujuan dan sasaran dari keamanan informasi.

Secara umum terdapat lima manfaat dari adanya tatakelola keamanan informasi ialah yang pertama, tercapainya kesesuaian (*alignment*) antara strategi keamanan informasi dan strategi bisnis. Kedua, perusahaan dapat melakukan pengelolaan risiko secara baik, dengan melakukan penilaian dan mitigasi risiko. Ketiga, penggunaan sumber daya yang terkelola secara efektif dan efisien untuk mencapai tujuan dan sasaran keamanan informasi. Keempat, pengukuran terhadap keberhasilan pelaksanaan keamanan informasi dapat dilakukan. Kelima, optimalisasi nilai manfaat dan investasi yang digunakan untuk mencapai tujuan dan sasaran keamanan informasi.



Gambar 2.13 Konsep Tatakelola Keamanan Informasi

Pada gambar diatas dijelaskan bahwa, konsep tatakelola keamanan informasi diawali dari arahan senior management mengenai strategi bisnis dan sasaran organisasi, untuk menyusun kebutuhan keamanan informasi.

Kebutuhan keamanan informasi, juga dapat diperoleh dari hasil pengelolaan risiko, yang terdiri dari penilaian dan mitigasi risiko. Penilaian risiko akan melakukan analisis terhadap kondisi keamanan informasi perusahaan kondisi, sehingga dapat mengidentifikasi kerawanan/kelemahan, ancamana, kecenderungan dan dampak dari risiko, dan selanjutnya dinilai tingkat risikonya, serta rekomendasi kontrol keamanan untuk menurunkan risiko. Sedangkan tahap mitigasi risiko akan melakukan evaluasi dan analisis terhadap kontrol yang direkomendasikan, untuk selanjutnya merancang implementasi kontrol keamanan informasi.

BAB 4 PROFIL DAN PENILAIAN RISIKO

4.1 Profil Perusahaan

Pada bagian profil perusahaan, menjelaskan tentang sekilas perusahaan, visi misi perusahaan, struktur organisasi, bisnis inti yang dimiliki oleh PT. Multi Terminal Indonesia sebagai tempat studi kasus penelitian ini.

4.1.1 Sekilas Perusahaan

PT. Multi Terminal Indonesia (PT.MTI) adalah anak perusahaan PT (Persero) Pelabuhan Indonesia II (PELINDO II) yang memiliki bisnis inti (*core business*) pelayanan jasa bongkar muat barang.

PT. MTI merupakan *spin off* dari Divisi Usaha Terminal (DUT) yang sebelumnya adalah salah satu divisi di bawah komando PT PELINDO II Cabang Tanjung Priok. Maksud dan tujuan pendirian PT. MTI adalah dalam rangka mengoptimalkan potensi bisnis dan memperkuat *competitive advantage* sebagai *service provider*. Dari aspek legalitas, pendirian PT. MTI disahkan oleh Notaris Herdimansyah Chaidirsyah SH di Jakarta pada tanggal 15 Februari 2002 dengan komposisi kepemilikan saham P MTI adalah 99% milik PT PELINDO II dan 1% dimiliki olek Koperasi Pegawai Maritim (KOPEGMAR) Tanjung Priok.

Secara kronologis perubahan status dan bentuk perusahaan pelabuhan dibagi ke dalam beberapa periode sebagai berikut :

1. Periode 1960 – 1963

   Pengelolaan pelabuhan umum dilakukan oleh Perusahaan Negara (PN) Pelabuhan I sampai VIII berdasarkan Undang-Undang Nomor 19 prp tahun 1960.

2. Periode 1964 – 1969

   Aspek komersial dari pengelolaan pelabuhan dilakukan oleh PN Pelabuhan, sedangkan kegiatan operasional pelabuhan dikoordinasikan oleh Lembaga Pemerintah yang disebut Port Authority.

3. Periode 1969 – 1983

   PN Pelabuhan dan Port authority bergabung menjadi Badan Pengusahaan Pelabuhan (BPP) untuk mengelola pelabuhan umum berdasarkan PP Nomor 18 tahun 1969.

4. Periode 1984 – 1992

   Pengelolaaan pelabuhan umum yang diusahakan dilakukan oleh Perusahaan Umum (PERUM) Pelabuhan, sedangkan pengelolaan pelabuhan umum yang tidak diusahakan dilakukan oleh Unit Pelaksana Teknis (UPT) di bawah Direktorat Jenderal Perhubungan Laut sebagaimana diatur PP nomor 11 tahun 1983.

   PERUM Pelabuhan dibagi menjadi PERUMPEL I s/d IV dan Cabang Pelabuhan Tanjung Priok (Divisi Usaha Terminal) berada di bawah PERUMPEL II.

5. Periode 1992 – 2002

   Status PERUMPEL II berubah menjadi PT. (Persero) Pelabuhan Indonesia II sesuai dengan PP nomor 57 tanggal 19 Oktober 1991, dalam periode ini kegiatan bongkar muat masih tetap dilaksanakan oleh Divisi Usaha Terminal Cabang Pelabuhan Tanjung Priok.

6. Periode 2002 – sampai sekarang

   Divisi Usaha Terminal (DUT) dipisahkan (Spin Off) dari Cabang Pelabuhan Tanjung Priok menjadi PT. Multi Terminal Indonesia (PT.MTI).

Wilayah usaha PT. Multi terminal Indonesia berada di Pelabuhan Tanjung Priok Jakarta Utara.

4.1.2 Visi dan Misi Perusahaan

PT. Multi Terminal Indonesia memiliki visi "Menjadi perusahaan logistik terkemuka di Indonesia dengan penyediaan fasilitas dan pelayanan terpercaya kepada pelanggan".

Sesuai dengan visi tersebut, PT. MTI mempunyai misi, antara lain:

- Melayani sistem distribusi muatan kapal di pelabuhan dengan bongkar muat serta penumpukan dengan efisien dan aman;
- Mendukung pelayanan kepelabuhanan yang efisien untuk menjamin daya saing perdagangan.
- Memupuk keuntungan berdasarkan prinsip pengelolaan perusahaan.
- Mewujudkan sumber daya manusia yang profesional dan mampu berkembang untuk memenuhi permintaan pasar.

Sedangkan maksud dan tujuan pendirian PT. MTI seperti yang diuraikan sebelumnya adalah dalam rangka mengoptimalkan potensi bisnis dan memperkuat *competitive advantage* sebagai *service provider*.

4.1.3 Struktur Organisasi

Sumber Daya Manusia sebagai penggerak utama jalannya perusahaan, menjadi prioritas utama PT. MTI dalam meningkatkan kualitas dan kemampuan SDM, melalui pendidikan dan pelatihan baik di dalam maupun luar negeri, penjenjangan manajerial, teknis subtansial, seminar, lokakarya dan sejenisnya menjadi agenda terjadwal dan terancang dengan baik. Terhadap pekerja potensial yang memiliki integritas dan kemauan mengembangkan diri, diberikan kesempatan untuk menambah pengetahuan, *skill* dan wawasan kepelabuhanan melalui program-program yang telah disiapkan, sehingga tercipta SDM yang unggul dan profesional di bidangnya.

Struktur organisasi PT. MTI digambarkan sebagai berikut.

Gambar 4.1 Struktur Organisasi PT. Multi Terminal Indonesia

PT MTI menyadari sepenuhnya jumlah SDM masih kurang memadai, bila dibanding dengan cakupan layanan yang diberikan kepada pengguna jasa. Oleh karena itu kerjasama yang baik dengan mitra usaha akan mampu meningkatkan pendapatan (*revenue*) secara maksimal dengan upaya yang lebih efisien. Beberapa mitra kerja PT. MTI memiliki keahlian yang spesifik sesuai dengan bidangnya masing-masing.

4.1.4 Bisnis Inti

Ruang lingkup kegiatan pelayanan perusahaan saat ini dapat dikelompokkan menjadi 3 unit strategis (Strategic Business Unit) yang meliputi:

- *Multipurpose Terminal*
- *Container Terminal*
- *Freight Forwarding*

Terminal Serbaguna (Multipurpose Terminal)

Sebagai Terminal Operator (TO), PT. MTI berupaya untuk mengembangkan cakupan pelayanan dan penetrasi pasar dengan merespons keinginan pelanggan dengan berusaha memberikan layanan yang cepat, aman dan murah serta penyediaan fasilitas Terminal Multipurpose untuk melayani dan menangani kegiatan bongkar muat barang peti kemas dan non petikemas *(Bulk Cargo, General Cargo, CPO* dan *life stock*)

Tarif yang bersaing, jaminan keamanan dan layanan kegiatan operasional 24 jam sehari, merupakan salah satu bentuk penawaran yang diberikan kepada para pelanggan, dalam rangka meningkatkan mutu pelayanan. Upaya lain yang dilakukan adalah menciptakan value creation, dengan melakukan beberapa inovasi metode penanganan bongkar muat semen curah dan *klinker*. Metode baru ini telah terbukti berhasil meningkatkan *Ship Output Per-day* (SOP) dari semula 7000 ton/day menjadi 22.000 ton/day. Karena prestasi ini, PT. MTI mendapatkan penghargaan dari pengguna jasa atas *performance* yang telah dicapai sehingga PT. MTI menjadi PBM dengan SOP tertinggi di kawasan Asia Tenggara khususnya untuk penanganan bongkar muat semen curah dan *klinker*.

Container Terminal

Container Terminal Regional Harbour (TPRH) merupakan pengembangan dari terminal serbaguna (*Multipurpose Terminal*) yang ketika itu dibangun khusus menangani bongkar muat petikemas antarpulau, setelah menjadi bagian dari PT. MTI, Container Terminal diharapkan dapat menjadi terminal petikemas yang mempunyai lingkup usaha lebih luas lagi tidak saja regional tetapi juga berskala internasional. Container Terminal segera berbenah diri dengan melakukan pengembangan peningkatan kerjasama usaha dengan pihak swasta nasional dalam rangka penyediaan alat bongkar muat.

Seiring dengan perkembangan teknologi informasi selain pemanfaatan aplikasi CTOS *(Container Terminal Operation System),* saat ini TPRH juga telah dilengkapi teknologi *wireless system* dengan menggunakan *handheld* untuk mendukung kegiatan operasional sehingga data dan informasi menjadi lebih akurat dan real time.

Freight Forwarding

Fasilitas dan peralatan yang dimiliki Divisi Freight Forwarding antara lain fasilitas lapangan penumpukan (*open storage*), gudang konsolidasi dan distribusi barang ekspor-impor (CCC/CDC), layanan petikemas interinsuler dan Terminal Petikemas Pasoso yang melayani angkutan petikemas dengan menggunakan kereta api dari dan ke Stasiun Gede Bage Bandung.

Profil perusahaan yang telah dijelaskan diatas, dapat memberi gambaran tentang bagaimana PT. MTI, dalam melakukan bisnisnya, dengan sumber daya yang dimilikinya. Sebelum melakukan penilaian risiko berdasarkan sember daya dan aset-aset kritikal yang dimiliki oleh perusahaan, maka perlu ditentukan sasaran keamanan informasi, yang akan capai, sehingga penilaian risiko yang dilakukan akan lebih fokus dan searah dengan kebutuhan penyusunan rancangan keamanan informasi perusahaan.

4.2 Penentuan Tujuan dan Sasaran Rancangan Keamanan Informasi

Rancangan keamanan yang akan disusun berdasarkan hasil penilaian dan mitigasi risiko, harus memiliki tujuan dan sasaran, karena hal ini akan membuat proses identifikasi risiko menjadi lebih lebih fokus.

Tujuan utama yaitu dapat melakukan pencegahan (*preventive*) dari risiko, pengurangan (*reduce*) risiko dan pengembalian atau respon terhadap gangguan atau bencana (*respond and recovery*). Berdasarkan tujuan tersebut, maka akan dapat diturunkan menjadi beberapa sasaran, sebagai berikut:

a. Dapat menentukan kebijakan yang dibutuhkan dalam mendukung implementasi keamanan informasi.
b. Dapat mengidentifikasi aset-aset perusahaan yang sensitif dan kritikal milik perusahaan, serta mengidentifikasi risiko, ancaman dan kerawanannya.
c. Dapat mengidentifikasi pengelolaan Sumber Daya Manusia (SDM) dalam mendukung keamanan informasi
d. Dapat mengidentifikasi pengelolaan fisik dan lingkungan keamanan informasi.
e. Dapat mengidentifikasi pengelolaan komunikasi dan operasional keamanan informasi.
f. Dapat mengidentifikasi pemeliharaan pada perangkat dan sistem, yang perlu dilakukan untuk menjamin keamanan informasi.
g. Dapat mengidentifikasi pengelolaan insiden keamanan informasi yang berpotensi terjadi.
h. Dapat mengidentifikasi pengelolaan keberlanjutan bisnis, yang perlu dilakukan.

Berdasarkan tujuan dan sasaran rancangan keamanan informasi diatas, maka akan dilakukan penilaian risiko yang akan menjadi rekomendasi bagi rancangan keamanan informasi. Di bawah ini merupakan target dari proses penilaian risiko, ialah:

a. Adanya usulan kebijakan keamanan informasi.
b. Terdapat Informasi tentang aset-aset perusahaan yang kritikal, serta kontrol yang dapat digunakan untuk menjaga keamanan informasi.
c. Disampaikannya usulan dalam pengelolaan SDM untuk penerapan keamanan informasi.

d. Adanya rekomendasi kontrol dalam pengelolaan fisik dan lingkungan Keamanan Informasi.
e. Usulan cara mengkomunikasikan dan menjalankan kebijakan keamanan informasi.
f. Adanya usulan dalam proses pembangunan sistem dan pemeliharaan, yang perlu dilakukan.
g. Terdapat informasi tentang insiden keamanan informasi yang berpotensi terjadi.
h. Disampaikannya usulan kontrol untuk menjaga keberlanjutan bisnis.

Tujuan dan sasaran rancangan keamanan informasi diatas, selanjutnya akan menjadi acuan dalam melakukan penilaian risiko berdasarkan kondisi *existing* perusahaan. Penilaian risiko akan fokus pada sembilan domain tujuan dan sasaran diatas, sehingga mampu memberikan bahan dalam penyusunan rancangan keamanan berdasarkan penilaian dan mitigasi risiko.

Sasaran keamanan informasi akan menjadi arahan untuk melakukan penilain risiko, sehingga lingkup dari aspek penilaian sesuai dengan sasaran yang ingin dicapai dalam penyusunan rancangan keamanan informasi perusahaan. Selanjutnya akan dilakukan penilaian risiko terhadap PT. MTI sebagai studi kasus penelitian. Penjelasan tentang pelaksanaan penilaian risiko akan disampaikan pada bagian selanjutnya.

4.3 Kegiatan Penilaian Risiko

Berdasarkan uraian sebelumnya mengenai penilaian risiko keamanan informasi (*risk assessment*), maka pada bagian ini akan dilakukan observasi dan wawancara kepada pihak internal perusahaan yang terkait dengan pengelolaan teknologi informasi.

Daftar materi pertanyaan untuk observasi dan wawancara ini dapat dilihat pada bagian lampiran laporan. Adapun langkah-langkah yang akan dilakukan dalam penilaian risiko TI, sebagai berikut:

1. Karakteristik Sistem, yaitu melakukan identifikasi karakteristik sistem yang digunakan oleh perusahaan (*system characterization)*
2. Identifikasi ancaman, yaitu melakukan identifikasi ancaman terhadap aset yang dimiliki (*threat identification)*
3. Identifikasi Kelemahan/Kerawanan (*vulnerability determination)*
4. Analisis Kontrol (*control analysis)*
5. Penilaian Kecenderungan (*Likelihood determination)* dan Analisis Dampak (*impact analysis)*
6. Pengenalan dan Tingkat Risiko (*risk determination)*
7. Rekomendasi Kontrol (*control recommendation)*

Hasil yang diperoleh dari setiap tahapan penialian risiko, akan diuraikan pada bagian selanjutnya.

4.4 Karakteristik Sistem

Dalam mengidentifikasi risiko keamanan informasi, sangat membutuhkan pemahaman yang baik, tentang lingkungan sistem TI yang ada pada perusahaan tersebut, maka perlu dilakukan identifikasi karakteristik sistem pada perusahaan.

Identifikasi karakteristik sistem yang akan dilakukan, harus mengacu pada domain tujuan dan sasaran rancangan keamanan, sehingga akan diperoleh risiko terkait domain tersebut, dan selanjutnya akan dibuat tindakan mitigasi risiko, yang akan menjadi acuan dalam penyusunan rancangan keamanan.

Berdasarkan tujuan dan sasaran yang telah ditetapkan, maka terdapat sembilan proses yang harus diidentifikasi pengelolaannya, karena sangat terkait dengan risiko keamanan informasi yang dapat ditimbulkan. Adapun sembilan proses tersebut ialah:

a. Pengelolaan kebijakan keamanan informasi
b. Pengelolaan aset perusahaan
c. Pengelolaan SDM keamanan informasi
d. Pengelolaan fisik dan lingkungan keamanan informasi
e. Pengelolaan komunikasi dan operasional
f. Pengelolaan pembangunan sistem dan pemeliharaannya
g. Pengelolaan insiden keamanan informasi
h. Pengelolaan keberlanjutan bisnis

Penjelasan dari sembilan sasaran diatas, adalah:

- Pengelolaan kebijakan keamanan informasi, yaitu proses penyusunan kebijakan keamanan informasi, dan upaya untuk menjalankan segara aturan tersebut, yang bertujuan menjaga keamanan informasi perusahaan.
- Pengelolaan aset perusahaan, yaitu proses untuk menjaga aset teknologi informasi yang dimiliki perusahaan, agar dapat tetap terjaga kerahasiaannya, integrasi dan ketersediaannya.
- Pengelolaan SDM keamanan informasi, yaitu proses perekrutan, pelatihan dan penugasan tenaga personil agar dalam menjalankan tugasnya dapat memperhatikan keamanan informasi.
- Pengelolaan fisik dan lingkungan keamanan informasi, yaitu proses pemeliharaan dan perawatan peralatan dan perlengkapan TI, agar tida mengganggu keamanan informasi
- Pengelolaan komunikasi dan operasional keamanan informasi, yaitu proses sosialisasi dan upaya untuk meningkatkan kepedulian karyawan perusahaan untuk menjaga keamanan informasi.
- Pengelolaan pembangunan sistem dan pemeliharaannya, yaitu proses pembangunan dan pemeliharaan sistem aplikasi dan perangkat lunak agar tetap memenuhi keamanan informasi.
- Pengelolaan insiden keamanan informasi, yaitu proses pendokumentasian dan analisis terhadap kejadian gangguan dan serangan yang dapat mengganggu keamanan informasi.

- Pengelolaan keberlanjutan bisnis, yaitu proses penyusunan rancangan untuk menjaga keberlanjutan bisnis, saat terjadi bencana atau kejadian darurat, agar bisnis tetap bisa berjalan.

Berdasarkan sembilan proses yang akan diidentifikasi potensi risikonya, maka ditentukan secara detail ceklis untuk setiap proses diatas. Ceklist ini akan menjadi isi dari bahan observasi dan wawancara dalam penilaian risiko. Berikut ini detail ceklis untuk setiap proses:

1. Pengelolaan kebijakan keamanan informasi: akan diperoleh informasi tentang:
   - Ada/tidaknya kebijakan kemanan informasi
   - Ada/tidaknya arsitektur kemanan informasi
2. Pengelolaan aset perusahaan: akan diperoleh informasi tentang:
   - Identifikasi aset fisik : seperti gedung, komputer, dan lain-lain
   - Identifikasi aset jaringan dan komunikasi: jaringan komputer
   - Identifikasi aset software dan aplikasi: perangkat lunak dan aplikasi yang digunakan dalam menjalankan proses bisnis.
   - Identifikasi aset informasi: data dan informasi yang sensitif dan kritikal
   - Identifikasi aset personil: pegawai yang bekerja di perusahaan.
   - Identifikasi aset sarana pendukung: listrik, air, pengatur udara, dan lain-lain
3. Pengelolaan Sumber Daya Manusia (SDM) Keamanan Informasi: akan diperoleh informasi tentang:
   - Jumlah personil yang terlibat untuk mengontrol keamanan informasi
   - Informasi tantang keahlian dan pendidikan personil TI.
4. Pengelolaan fisik dan lingkungan Keamanan Informasi: akan diperoleh informasi tentang:
   - Bagaimana pengelolaan gedung dan ruang khusus IT.
   - Kerentanan terhadap gangguan dari bencana alam (gempa bumi, banjir, petir), dan gangguan manusia (kerusahan, kebakaran dan lain-lain)

5. Pengelolaan komunikasi dan operasional keamanan informasi: akan diperoleh informasi tentang:
   - Kegiatan sosialisasi akan kemanan informasi kepada para pegawai/karyawan perusahaan
   - Apakah prosedur keamanan informasi dijalankan oleh pada pegawai/karyawan perusahaan.
6. Pengelolaan pembangunan sistem dan pemeliharaannya: akan diperoleh informasi tentang:
   - Ada/tidak nya fungsi keamanan informasi pada aplikasi yang dibangun.
   - Ada/tidaknya dilakukannya pengujian dan pemeliharaan terhadap sistem akan kerentanan gangguan dan kelemahannya.
7. Pengelolaan insiden keamanan informasi: akan diperoleh informasi tentang:
   - Ada/tidaknya sistem pencatatan kejadian terkait dengan keamanan informasi
   - Ada/tidaknya dilakukan analisis dan tindakan terhadap kejadian tersebut.
8. Pengelolaan keberlanjutan bisnis: akan diperoleh informasi tentang:
   - Ada/tidaknya rancangan untuk tetap menjaga keberlangsungan bisnis, jika terjadi gangguan terhadap sistem
   - Kesiapan peralatan dan perlengkapan untuk menjaga keberlangsungan bisnis, jika terjadi gangguan terhadap sistem.

Detail proses diatas, akan menjadi bahan observasi dan wawancara dalam penilaian risiko, yang hasil-hasilnya akan dibahas pada bagian selanjutnya.

4.4.1 Pengelolaan Kebijakan Keamanan Informasi

Pada kegiatan observasi dan wawancara telah ditanyakan, mengenai kebijakan keamanan informasi yang dimiliki oleh perusahaan, maka diperoleh hasil bahwa perusahaan telah memiliki *program policy*, *standar access definition policy*, *password management policy*, *internet usage policy*, *network security policy*, *remote access policy*, *server platform policy* dan *application security policy*, tetapi hanya *internet usage policy* yang hanya secara tertulis telah ditetapkan.

Tabel 4.1 Kebijakan Keamanan Informasi Perusahaan

Policy	Ada	Tidak	Keterangan
Program Policy	√		Tidak lengkap (tanpa detection)
Information/Resource Classification		√	
Standard Access Definition Policy	√		Belum tertulis
Password Management Policy	√		Password diberikan oleh Admin
Internet Usage Policy	√		surat permohonan dari pimpinan
Network Security Policy	√		Belum tertulis
Remote Access Policy	√		Belum tertulis
Dekstop Policy		√	
Server Platform Policy	√		Belum tertulis
Application Security Policy	√		Belum tertulis

Selanjutnya, telah ditanyakan pula tentang perancangan arsitektur keamanan informasi di perusahaan, tetapi diperoleh hasil bahwa perusahaan tidak memiliki perancangan yang tertulis tentang arsitektur keamanan informasinya.

Tabel diatas menjelaskan bahwa terdapat kelemahan/kerawanan yang dimiliki perusahaan, sebagai berikut:

- Perusahaan telah memiliki beberapa kebijakan yang sangat dibutuhkan dalam rangka keamanan informasi, seperti kebijakan program, standar akses, manajemen password, penggunaan password dan internet, kebijakan keamanan jaringan, remote akses, server dan kebijakan keamanan aplikasi. Tetapi kebijakan tersebut tidak diformalkan dalam sebuah dokumen kebijakan TI, sehingga hal ini merupakan kelemahan/kerawanan (*vulnerabilities*) yang dimiliki perusahaan.
- Perusahaan belum memiliki kebijakan mengenai penggunaan dekstop komputer, dan pengklasifikasian aset dan informasi, dan hal ini merupakan kelemahan/kerawanan (*vulnerabilities*) yang dimiliki perusahaan.

Analisis dari tabel tersebut, bahwa kelemahan/kerawanan yang telah disebutkan diatas, berpotensi menimbukan risiko, sebagai berikut:

1. Kebijakan keamanan yang tidak diformalkan sebagai sebuah kebijakan perusahaan, akan berpotensi menimbulkan resiko keamanan informasi, diataranya:
   - Risiko terganggunya keamanan informasi.
     Jika perusahaan memiliki karyawan baru yang menempati posisi strategis dan taktis, maka karyawan tersebut tidak akan pernah mengetahui tentang kebijakan perusahaan dalam pengamanan informasinya, sehingga berpotensi resiko terganggunya keamanan informasi.
   - Risiko ketidaksesuaian dan pelangaran kebijakan.
     Pengadaan atau implementasi teknologi baru pada perusahaan, tidak disadari melanggar atau tidak sesuai dengan kebijakan keamanan informasi yang berlaku di perusahaan.

2. Tidak adanya kebijakan dekstop akan menimbulkan risiko, sebagai berikut:
   - Risiko kehilangan informasi, modifikasi informasi dan pencurian informasi melalui komputer yang tidak terbuka, saat pemiliknya tidak berada ditempat.
3. Tidak adanya kebijakan tentang pengklasifikasian aset/informasi, akan menimbulkan resiko, sebagai berikut:
   - Risiko hilangnya kerahasiaan informasi, karena informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka.

4.4.2 Pengelolaan Aset Perusahaan

Pengelolaan aset perusahaan akan mengidentifikasi mengenai aset-aset yang dimiliki oleh perusahaan saat ini. Aset-aset tersebut antara lain aset fisik, jaringan dan komunikasi, software dan aplikasi, data dan informasi, personil dan sarana pendukung.

4.4.2.1 Aset Perangkat Keras

Berdasarkan hasil observasi dan wawancara, maka diperoleh informasi mengenai perangkat keras yang dimiliki oleh perusahaan, sebagai berikut:

1. Terdapat 152 Unit Personal Computer (PC)
2. Terdapat 19 unit Server yang tersebar pada unit bisnisnya, dengan rinciannya: TPK : 3 unit, CDC : 2 unit, PSS : 1 unit, dan KP: 19 unit

Adapun spesifikasi Server dan PC, sebagai berikut :

Tabel 4.2 Spesifikasi Server

Port Number	433525-371
Form Factor	2U Rack
Processor	Intel Xeon E5335 Quad Core Processor: 2 GHz, 2x 4 MB L2 Cache, 1333 FSB
Number of Processor	1
Upgrade processor	Upgradeable to 2 processor
Memory Type	PC2-5300 DDR2-667 with advanced ECC, mirror, and online spare memory capabilities
Std Memory Max	2x 1 GB (32 GB)
Memory Type	8 DIMM slot
Internal HDD	None
Hard Disk Controller	Smart Array P400/256 Controller (RAID 0/1/1 +0/5)
Internal Drive Bays	SFF (2.5") SAS/SATA HDD Bays
Network Interface	Embendded Dual NC373i Multifunction Gigabit Server Adapter with TCP/IP Offload Engine
Optical Drive	Optional
Expansion Slot	4x PCI-E slot (optional mixed PCI-X/PCI-E Configuration)
Port	1x Serial, Mouse, Graphic, Keyboard, 2x VGA (front, & back)
Power Management	800 Watt (optional AC Redundance Power Supply)
OS Supported	- Microsoft Windows Server 2000 - Microsoft Windows - Server 2003 - Novell Netware - Red Hat Enterprise Linux - SUSE Linux Enterprise Server - SCO UnixWare, Open Server - Vmware Virtualization Software - Solaries 10 32/64-bit

Tabel 4.3 Spesifikasi PC

Processor	Core 2 Duo Intel
RAM	1 GB
Storage	250 GB
Motherboard	Asus
VGA	On Board

Tabel diatas dapat menjelaskan bahwa aset fisik berupa server dan komputer, memiliki spesifikasi yang khusus dan memadai.

- Harga server dengan spesifikasi diatas sekitar US$ 3,775 atai Rp.45.300.000 ($1 = Rp.12.000,-).
- Harga 1 komputer dengan spesifikasi diatas sekitar US$ 899 atau Rp. 10.788.000

Analisis dari data mengenai aset server dan komputer diatas, bahwa:

- Pembiayaan pergantian perangkat, dengan spesifikasi tersebut, akan membutuhkan biaya yang cukup besar, untuk perbaikan atau pergantiannya, jika terjadi kehilangan atau kerusakan.

4.4.2.2 Aset Perangkat Lunak

Berdasarkan hasil observasi dan wawancara, maka diperoleh informasi mengenai perangkat lunak yang digunakan oleh perusahaan, sebagai berikut:

a. Sistem Operasi yang digunakan pada PC dan Server

Di bawah ini merupakan sistem operasi yang digunakan pada PC dan server di perusahaan:

Tabel 4.4 Sistem Operasi yang digunakan

Sistem Operasi PC	Sistem Operasi SERVER
Windows XP	Windows 2000
Windows 98	Windows 2003
Windows Vista	Unix SCO

Tabel diatas menjelaskan bahwa:

- Perusahaan menggunakan sistem operasi yang berlisensi dan *open source*. Pengumaan sistem operasi berlisensi selain mahal, juga cukup rentan dengan infeksi virus.
- Penggunaan sistem operasi open source, tidak hanya untuk efisiensi biaya, tetapi diharapkan dapat lebih handal dalam operasional khususnya server.

Analisis dari data diatas, sebagai berikut:

- Penggunaan sistem operasi, yang rentan dengan gangguan virus, tanpa didukung oleh perangkat antivirus yang cukup handal, ialah dapat menimbulkan kerusakan file, dan kehilangan file data.
- Penggunaan sistem operasi yang open source, ialah dibutuhkannya keterampilan dan pengetahuan yang cukup bagi para karyawan di bidang TI di perusahaan, agar dapat melakukan konfigurasi dari sistem operasi open source tersebut.

b. Perangkat lunak perkantoran yang digunakan (*software*)

Di bawah ini merupakan perangkat lunak perkantoran yang digunakan di perusahaan:

Tabel 4.5 Perangkat lunak perkantoran yang digunakan

No	Aplikasi Pendukung Perkantoran
1	Microsoft office 97
2	Microsoft Office 2003, XP
3	Microsoft XP
4	Email Server multiterminal.co.id

Tabel diatas menjelaskan bahwa:

- Perusahaan menggunakan aplikasi pendukung perkantoran yang secara umum digunakan.
- Serta penggunaan email sebagai media komunikasi kepada internal dan eksternal.

Analisis dari data diatas:

- Penggunaan mail server, berpotensi sebagai pintu masuknya virus dan trojan, yang harus dapat mengganggu
- Penggunaan mail server lainnya, ialah kecenderungan mudah dimasuki oleh para hacker, karena biasanya perusahaan menggunakan mail server yang banyak dipasaran.

c. Perangkat lunak pendukung bisnis yang digunakan (software)

Di bawah ini merupakan perangkat lunak pendukung bisnis yang digunakan di perusahaan:

Tabel 4.6 Perangkat lunak pendukung bisnis yang digunakan

No	Nama Sistem Aplikasi	Deskripsi
1	CTOS	Sistem petikemas
2	Warehouse	Sistem pergudangan
3	TO	Sistem Terminal Operator
4	Ship & Yard Plan	Sistem Perencanaan Lapangan
5	Forwarding	Sistem Forwarding
6	TPK Pasoso	Sistem petikemas kereta api
7	SIMKEU	Sistem Informasi Keuangan
8	SMPERS	Sistem Informasi Personalia

Tabel diatas menjelaskan bahwa:

- Perusahaan membangun aplikasi-aplikasi yang dapat mendukung proses bisnisnya, dengan fungsionalitas yang disesuaikan dengan kebutuhan dilapangan, dimana pembangunan aplikasi-aplikasi tersebut mengunakan pihak luar atau perusahaan pembuat aplikasi.

Analisis data diatas, sebagai berikut;

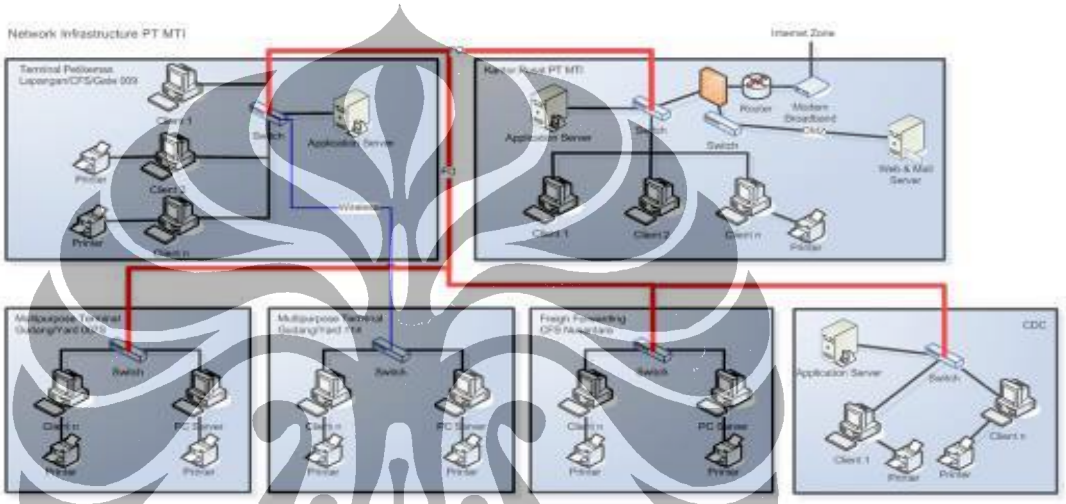
- Potensi integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi antar data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai.

4.4.2.3 Aset Jaringan dan Komunikasi

Berdasarkan hasil observasi dan wawancara, maka diperoleh informasi mengenai jaringan dan komunikasi yang digunakan oleh perusahaan, sebagai berikut:

1. **Topologi Jaringan Komputer**

   Di bawah ini merupakan topologi dari jaringan komputer yang dimiliki oleh perusahaan:



Gambar 4.2 Topologi Jaringan Komputer Perusahaan

Gambar topologi diatas menjelaskan bahwa;

- Aset data dan informasi perusahaan yang berada di server, hanya dilindungi oleh satu firewall saja.
- Perusahaan telah menggunakan media kabel fiber optic, yang akan mempercepat transmisi data antar jaringan di internal.

Analisis dari gambar tersebut, sebagai berikut:

- Potensi adanya penyusupan dan gangguan yang berasal dari jaringan lokal, disebabkan oleh penggunaan firewall pada sisi luar jaringan saja, berpotensi terbukanya wilayah server dari gangguan yang berasal dari dalam jaringan (lokal).

2. Koneksi Internet

Perusahaan ini menggunakan leased line untuk koneksi internet dengan memilih providernya yaitu Telkom.

3. Perangkat Jaringan Komputer

Di bawah ini merupakan perangkat jaringan komputer yang dimiliki oleh perusahaan:

Tabel 4.7 Perangkat Jaringan Komputer

Perangkat	Ada	Tidak
Router	√	
Switch	√	
Access Point (wireless)	√	
Modem	√	
Perangkat VPN (Virtual Private Network)		√

Tabel diatas menjelaskan bahwa perangkat jaringan yang dimiliki oleh perusahaan ialah router, switch, access point dan modem, sedangkan VPN tidak digunakan.

4. Fasilitas Internet yang digunakan

Di bawah ini merupakan fasilitas internet yang digunakan oleh perusahaan:

Tabel 4.8 Fasilitas Internet yang digunakan

Perangkat	Ada	Tidak
World wode web (www)	√	
Email	√	
File Transfer Protocol (FTP)		√
Remote Access	√	

Tebel diatas menjelaskan bahwa fasilitas internet yang digunakan perusahaan, ialah *world wide web* (www), email, dan *remote access*, sedangkan *file transfer protocol* (FTP), tidak digunakan.

5. Penggunaan Protokol Internet

Di bawah ini merupakan protokol internet yang digunakan oleh perusahaan:

Tabel 4.9 Penggunaan Protokol Internet

Penggunaan IP	Ada	Tidak	Keterangan
IP Statis	√		Wireless Network tetap menggunakan IP static
DHCP		√	

Tabel diatas menjelaskan bahwa pada lingkungan jaringan komputer di perusahaan, mengunakan IP statis, pada koneksi wireless dan wire, sehingga DHCP tidak digunakan.

Analisis dari data tersebut sebagai berikut:

- Penggunaan IP statis dapat menurunkan resiko adanya penyusupan yang rentan menggunakan koneksi wireless, tetapi penggunaan IP statis berarti menjadikan informasi IP yang diperusahaan harus menjadi informasi yang rahasia (confidential).

6. Penggunaan Firewall

Di bawah ini merupakan firewall yang digunakan pada jaringan komputer perusahaan:

Tabel 4.10 Firewall yang digunakan

Jenis Firewall	Ada	Tidak
Personal Firewall: Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.		√
Network Firewall: Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server.	√	

Tabel diatas menjelaskan bahwa firewall, yang digunakan untuk melindungi jaringan komputer, adalah jenis network firewall, tetapi personal firewall yang merupakan fasilitas dari sistem operasi, secara umum tidak diaktifkan.

Analisis dari data diatas, sebagai berikut:

- Resiko masukkannya gangguan keamanan pada komputer personal cukup tinggi, karena tidak diaktifkannya firewall, hal ini disebabkan oleh tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.

4.4.2.4 Aset Informasi

Berdasarkan hasil observasi dan wawancara, maka diperoleh hasil identifikasi informasi yang sensitif dan kritikal di perusahaan , sebagai berikut:

Tabel 4.11 Identifikasi Informasi yang Sensitif dan Kritikal

Informasi	Confidentiality Low/Moderate/ High	Integrity Low/Moderate/ High	Availability Low/Moderate/ High
Informasi personalia (sallary)	L	H	H
Informasi Diskon/Tarif	H	H	H
Informasi Keuangan	H	H	H
Informasi Gudang (Durasi,Quantity)	L	H	H
Informasi di MPT (Durasi,Quantity)	L	H	H
Informasi FF (Durasi,Quantitiy)	L	H	H
Informasi configurasi jaringan	H	H	H

Tabel diatas menjelaskan bahwa:

- Terdapat informasi yang harus dijaga kerahasiaannya karena *confidentiality* dengan level "*high*", yaitu informasi tentang diskon dan tarif, serta informasi tentang konfigurasi jaringan, seperti IP.
- Terdapat pula informasi yang harus dijaga dari modifikasi yang tidak berhak serta harus menjamin ketersediaannya, seperti informasi personali, diskon/tarif, informasi gudang, informasi aplikasi.

Analisis dari data diatas, sebagai berikut:

- Resiko informasi dengan klasifikasi confidential tinggi, jika terbuka ke umum, berpotensi dapat menurunkan keuntungan dan citra perusahaan. Untuk itu Informasi yang terklasifikasi memiliki level kerahasiaan tinggi, harus memperoleh prioritas keamanan.

4.4.2.5 Aset Personil

Berdasarkan hasil observasi dan wawancara, maka diperoleh informasi tentang personil/karyawan yang bekerja di perusahaan , sebagai berikut:

Tabel 4.12 Komposisi Pekerja Berdasarkan Jabatan (*Company Profile PT. MTI*)

No	Tenaga Organik	Satuan	Jumlah
1	Manajer	Orang	7
2	Staf Ahli	Orang	2
3	Kepala Internal Audit	Orang	1
4	Assisten Manager	Orang	2
5	Supervisor	Orang	25
6	Pelaksana	Orang	47
	Jumlah		84
7	Tenaga Kontrak (Outsource)	Orang	120
	Jumlah Total	Orang	224

Tabel 4.13 Komposisi Pekerja Berdasarkan Pendidikan (*Company Profile PT. MTI)*

No	Pendidikan	Satuan	Jumlah
1	Pasca Sarjana	Orang	3
2	Sarjana	Orang	5
3	Sarjana Muda	Orang	24
4	SLTA	Orang	33
5	SLTP	Orang	19
	Jumlah	Orang	84

Tabel diatas menjelaskan bahwa

- Perusahaan memiliki total jumlah pegawai tetap ialah 84 orang pegawai, dan tenaga kontrak sebanyak 120 orang pegawai.
- Sumber daya manusia (SDM) yang dimiliki perusahaan berpendidikan pasca sarjana dan sarjana masih terbatas.

Analisis dari data tersebut

- Dengan jumlah pegawai 224 orang, maka perusahaan ini tergolong usaha besar, dengan jumlah karyawan lebih besar dari 100 orang.
- Dengan SDM berpendidikan pasca sarjana dan sarjana terbatas, maka perlu melakukan pelatihan secara rutin kepada karyawan, agar mampu menguasai teknologi dan memahami tatakelola keamanan informasi yang baik, untuk meningkatkan efisiensi dan efektifitas perngelolaan perusahaan.

4.4.2.6 Aset Sarana Pendukung

Aset sarana pendukung yang dimiliki oleh perusahaan, adalah peralatan dan perlengkapa pendukung gedung dan ruangan yaitu,

Tabel 4.14 Sarana Pendukung

Sarana Pendukung	Ada	Tidak	Keterangan
Pendingin ruangan (AC)	√		Pada setiap ruang dikantor kantor tersedia AC, dan tentunya pada ruang Server, tetapi belum memiliki jadwal pemeliharaan yang rutin.
Genset	√		Genset tersedia untuk ruang kantor (1 buah) dan untuk operasional di lapangan (1 buah).
Penerangan	√		Penerangan sudah cukup, sesuai dengan kebutuhan.

Tabel diatas menjelaskan bahwa

- Perusahaan telah memiliki sarana pendukung jalannya perangkat TI dalam mendukung proses bisnisnya, diantaranya pendingin ruangan (AC), genset, dan penerangan.

Analisis dari data tersebut, sebagai berikut:

- Adanya potensi komputer atau server menjadi rawan rusak karena suhu ruangan yang ringgi, sehingga perangkat pendukung diatas, menjadi sangat penting, karena sebagian besar operasional perusahaan, menggunakan perangkar komputer/server. Perangkat komputer dan server tersebut, harus didukung oleh pendinginruangan yang baik, agar tidak rentan dengan kerusahakan.

4.4.3 Pengelolaan Sumber Daya Manusia TI

Pengelolaan sumber daya manusia, akan mengetahui penugasan personil di bidang TI di perusahaan. Adapun informasi yang diperoleh sebagai berikut:

1. Divisi Sistem Informasi dan Pengadaan memiliki 2 (dua) karyawan sebagai Administrator , dimana satu orang berada di kantor, dan satu orang lagi berada dilapangan.
2. Sedangkan untuk pengguna (user) dari aplikasi-aplikasi yang berjalan, sebagai berikut:

Tabel 4.15 Pengguna Sistem Aplikasi pendukung bisnis

No	Nama Sistem Aplikasi	Jumlah Pengguna Aplikasi	Keterangan
1	CTOS	119 user	dengan 30 PC
2	Warehouse	30 user	dengan 15 PC
3	TO	10 user	dengan 5 PC
4	Shif & Yard Plan	6 user	dengan 2 PC
5	Forwarding	10 user	dengan 6 PC
6	TPK Pasoso	10 user	dengan 6 PC
7	SIMKEU	4 user	
8	SMPERS	4 user	

Tabel diatas menjelaskan bahwa :

- Tenaga TI di perusahaan terdiri dari Admin, teknisi dan operator aplikasi.
- Perusahaan memiliki tenaga operator aplikasi yang cukup banyak, dan kebanyakan dari mereka adalah tenaga kontrak.

Analisis dari data diatas:

- Dengan jumlah operator aplikasi yang banyak, maka diperlukan koordinasi yang baik dari koordinatornya.
- Operator, dengan jumlah yang cukup besar, yang mayoritas berstatus kontrak harian, perlu menjadi perhatian, karena sangat rentan dengan gangguan internal (insider).

4.4.4 Pengelolaan Fisik dan Lingkungan

Pengelolaan fisik dan lingkungan keamanan informasi, akan mengetahui informasi tentang peralatan dan perlengkapan yang dimiliki perusahaan yang digunakan sebagai pengaman aset informasi. Adapun informasi yang diperoleh sebagai berikut:

a. Gedung

Pada gedung milik perusahaan, terdapat ruang server atau data center, serta ruang DRC yang masih berada pada gedung yang sama.

Tabel 4.16 Pembagian Ruang TI

Ruangan	Ada	Tidak	Keterangan
Ruangan Server (data center)	√		Dibangun dengan alas panggung dan berkarpet.
Ruangan DRC	√		Satu lokasi dengan data center

Tabel diatas menjelaskan bahwa

- Perusahaan memiliki ruang khusus data center, dimana lokasi dari server database, aplikasi dan domain, dengan fasilitas ruangan data center seperti panggung, karpet, pendinginruangan, pencahayaan.
- Ruang DRC (Data Recovery Center), yang bertujuan menjadi backup dari data transaksi, masih berada pada ruang yang sama seperti data center.

Analisis dari data diatas, sebagai berikut:

- Resiko hilangnya data master dan backup berpotensi terjadi, karena ruang DRC yang seharusnya menjadi backup data dan menjamin keberlangsungan bisnis jika terjadi bencana pada ruang kantor, tidak dapat tercapai.

b. Lingkungan Lokasi Server/ data center

Pada gedung milik perusahaan, terdapat ruang server atau data center, serta ruang DRC yang masih berada pada gedung yang sama.

Tabel 4.17 Lingkungan Lokasi Server/Data Center

Data Center	Ya	Tidak	Keterangan
Natural Disaster Risks			
Data Center berada pada lokasi yang aman dari gangguan bencana alam (Banjir atau Gempa bumi), sehingga tidak diberada pada lantai bawah, atau paling atas)	√		
Man-Made Disaster Risks			
Data Center berada pada lokasi yang aman dari bencana yang bisa disebabkan oleh manusia, sehingga tidak berada pada tempat-tempat keramaian, seperti stadion,tepi jalan,dll)	√		
Infrastructure			
Electricity: power available untuk Komputer dan Server	√		
Terdapat pengatur suhu ruangan	√		
Pintu yang dapat dikunci	√		Pintu telah menggunakan finger print (access control)
Terdapat perangkat fire protection	√		Mengadung gas.
Penerangan (cahaya) yang cukup	√		
Ruangan yang aman dari Kelembaban dan debu	√		
Terdapat akses internet dengan bandwidth yang dibutuhkan	√		

Tabel diatas menjelaskan bahwa

- Ruang server/data center yang saat ini ada, telah memenuhi prasyarat sebuah data center, antara lain, bahwa data center tidak rawan terhadap bencana alam, karena berada pada lantai tiga (tidak di paling bawah, juga tidak di paling atas), juga jauh dari lokasi keramaian.
- Ruang server/data center juga memiliki sarana dan prasaranan yang memadai, seperti listrik, pendinginruangan, alat pemadam kebakaran, penerangan, serta akses internet. Pintu ruang data center juga telah dilengkapi oleh *finger print authentication*.

Analisis dari data diatas, sebagai berikut:

- Penggunaan finger print authentication dapat menjaga keamanan ruang server/data center dari masuknya orang yang tidak berhak.

4.4.5 Pengelolaan Komunikasi dan Operasional

Pengelolaan komunikasi dan operasional terkait dengan keamanan informasi, akan mengetahui kegiatan sosialisasi dan pelaksanaan prosedur keamanan informasi di perusahaan . Adapun informasi yang diperoleh bahwa sosialisasi keamanan informasi pernah dilakukan, tetapi tidak secara rutin, sehingga pergantian karyawan baru menyebabkan karyawan yang bekerja tidak mengetahui kebijakan atau prosedur keamanan informasi yang diterapkan oleh perusahaan.

Analisis dari data diatas, sebagai berikut:

- Terdapat potensi kurangnya informasi dan sosialisasi tentang keamanan informasi kepada para karyawan ialah, tidak adanya kesepakatan dan persamaan persepsi tentang bagaimana kebijakan perusahaan untuk menjaga keamanan informasinya.

4.4.6 Pengelolaan Pembangunan Sistem dan Pemeliharan

Pengelolaan pembangunan sistem dan pemeliharaannya akan mengetahui informasi penggunaan fungsi keamanan pada aplikasi dan pengujian serta pemeliharaan sistem . Adapun informasi yang diperoleh bahwa sosialisasi:

a. Fungsi keamanan informasi pada aplikasi yang dibangun, telah memiliki aspek keamanan, yaitu authentication dan authorization kepada penggunanya, tetapi belum menerapkan ekripsi pada data/informasi rahasia.
b. Perusahaan belum menerapkan pengujian keamanan sistem, seperti di bawah ini:

Tabel 4.18 Kontrol Fisik yang digunakan

No	System Security Testing	Telah Dilakukan	
		Ya	Tidak
1	Automated vulnerability scanning tools		√
2	Security test and evaluation		√
3	Penetration testing		√

c. Pemeliharaan terhadap sistem akan kerentanan gangguan dan kelemahannya, jarang dilakukan karena belum memiliki prosedur tertulis, sehingga pemeliharaan akan dilakukan hanya saat terjadi gangguan terhadap sistem.

Berdasarkan temuan diatas, dapat menjelaskan bahwa :

- Pembangunan aplikasi telah memperhatikan aspek keamanan seperti authentication dan authorization kepada penggunanya, tetapi karena belum mengimpelentasikan enkripsi pada data-datanya, sehingga risiko pencurian informasi oleh insiders berpeluang.

- Belum diterapkannya pengujian keamaanan sistem yang berjalan, menyebabkan tidak terukurnya kinerja sistem secara tepat, sehingga tidak dapat mengetahui kemampuan sistem yang suatu waktu akan tidak mampu lagi melayani pertambahan layanan yang semakin lama akan semakin besar.
- Pemeliharaan sistem dan perangkat yang tidak terjadwal dan tertulis dalam sebuah kebijakan, akan berisiko menimbulkan kelengahan dalam melakukan pemeliharaan tersebut, sehingga sistem dan perangkat dapat berpotensi akan terganggu keamanannya.

4.4.7 Pengelolaan Insiden Keamanan Informasi

Pengelolaan pembangunan sistem dan pemeliharaannya akan mengetahui informasi dilakukannya pencatatan, analisis dan tindakan terhadap insiden yang terjadi. Adapun informasi yang diperoleh bahwa tidak dilakukan pencatatan secara sistematis terhadap kejadian terkait dengan keamanan informasi, sehingga kejadian hanya dianalisis dan ditindak secara adhoc.

Analisis dari temuan diatas ialah:

- Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi, berpotensi internal perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, sehingga berpotensi satu saat nanti kelemahan tersebut diketahui orang, sehingga akan mengganggu keamanan informasi.

4.4.8 Pengelolaan Keberlangsungan Bisnis

Pada tahapan pengelolaan keberlangsungan bisnis, akan dijelaskan mengenai informasi tentang keberadaan rancangan darurat yang harus dijalankan jika terjadi gangguan terhadap sistem pendukung bisnis. Adapun informasi yang diperoleh bahwa perusahaan tidak memiliki rancangan penanggulangan bencana, agar bisnis dapat berjalan, meski terjadi bencana, yaitu dengan penyusunan BCP (*Business Continuity Plan)* dan DRP *(Data Recovery Plan)*. Sedangkan untuk *Disaster Recovery Center* (DRC) telah dimiliki saat ini, masih berada pada lokasi yang sama dengan data center, sehingga kerentanan keamanan informasi sangat tinggi.

Analisis dari temuan diatas, ialah:

- Rancangan penanggulangan bencana fokus pada bagaimana menjamin kontinuitas dari bisnis ketika kehilangan akses terhadap manusia, fasilitas, sistem informasi, layanan dan sumber daya lainnya, sehingga jika perusahaan tidak memiliki rancangan penanggulangan bencana, berpotensi terhentinya bisnis perusahaan.
- DRC yang terletak di lokasi yang sama dengan ruang server/data center, sangat berisiko tinggi terjadinya kehilangan data, karena jika terjadi bencana pada ruang server/data center, maka akan berakibat DRC pun mengalami hal yang sama, sehingga berpotensi bisnis dapat terhenti.

4.5 Identifikasi Ancaman

Threat-source akan sumber ancaman yang berpotensi dapat menyebabkan kerugian dari sistem TI perusahaan. *Thread-source* dapat berasal dari gangguan yang bersifat aktif dan pasif.

Tabel 4.19 Ancaman Aktif

No	Sumber Ancaman	Motivasi	Aksi yang dilakukan (* definisi dijelaskan pada LAMPIRAN form ini)	Pernah terjadi (Ya/Tdk)	Tingkat Kemungkinan Dapat Terjadi		
					High	Moderate	Low
1	**Hacker*, cracker***	• Challenge (ingin tantangan)	• Hacking	Y	√		
		• Ego	• Social engineering *	T		√	
			• System intrusion, break-ins (menyusup)	Y	√		
			• Unauthorized system access (akses tidak sah)	T			√
4	**Industrial espionage/Pengintai** (companies, foreign)	• Competitive advantage	• Economic exploitation (ekspoitasi/pemerasan)	T			√
		• Economic espionage	• Information theft (pencurial informasi)	T			√
			• Intrusion on personal privacy	T			√
			• Unauthorized system access (access to classified, proprietary, and/or technology-related information)	T		√	
5	**Insiders**	• Curiosity (keingintahuan)	• Assault on an employee (serangan dari pegawai)	T			√
		• Ego	• Blackmail *	T	√		
		• Intelligence	• Browsing of proprietary information	T	√		
		• Monetary gain (keuangan)	• Computer abuse (penyalahgunaan)	T			√
		• Revenge (balas dendam)	• Fraud and theft (penipuan dan pencurian)	T			√
		• Unintentional errors and omissions (e.g., data entry error, programming error)	• Information bribery (penyuapan)	T			√
			• Input of falsified, corrupted data (pemalsuan data)	T			√
			• Interception (pemotongan informasi)	T			√
			• Malicious code (e.g., virus, logic bomb, Trojan horse)	Y	√		
			• Sale of personal information (penjualan informasi)	T			√
			• System bugs (bug dari sistem)	Y	√		
			• System intrusion (penyusupan sistem)	T	√		√
			• System sabotage (sabotase sistem)	T			√
			• Unauthorized system access	T			√

Tabel 4.20 Ancaman Aktif (2)

No	Sumber Ancaman	Motivasi	Aksi yang dilakukan (* definisi dijelaskan pada LAMPIRAN form ini)	Pernah terjadi (Ya/Tdk)	Tingkat Kemungkinan Dapat Terjadi		
					High	Moderate	Low
2	**Computer criminal***	• Destruction of information	• Computer crime	T		√	
		• Illegal information disclosure	• Fraudulent (tidakan curang, seperti peniruan)	T			√
		• Monetary gain	• Information bribery (penyuapan)	T			
		• Unauthorized data alteration	• Spoofing *	T			
			• System intrusion (menyusup kedalam sistem)	T	√		
3	**Terrorist***	• Blackmail *	• Bomb/Terrorism	T			√
		• Destruction (kerusakan)	• Information warfare (Perang informasi)	T			√
		• Exploitation (eksploitasi)	• System attack (e.g., distributed denial of service) *	T	√		
		• Revenge (balas dendam)	• System penetration*	T	√		
			• System tampering*	T	√		

Tabel 4.21 Ancaman Pasif

No	Sumber Ancaman	Motivasi	Aksi yang dilakukan	Pernah terjadi (Ya/Tdk)	Tingkat Kemungkinan Dapat Terjadi		
					High	Moderate	Low
1	**Kegagalan perangkat lunak dan perangkat keras**		• Gangguan listrik	T	√		
			• Kegagalan peralatan	Y	√		
			• Kegagalan fungsi perangkat lunak	Y	√		
2	**Kesalahan manusia**		• Kesalahan pemasukan data	Y	√		
			• Kesalahan penghapusan data	Y	√		
			• Kesalahan operator	Y	√		
3	**Alam/Bencana Alam**		• Gempa Bumi	T			√
			• Banjir	T			√
			• Kebakaran	T			√
			• Petir	Y	√		
4	**Lingkungan**		• Goncangan tanah				

Berdasarkan informasi dari tabel ancaman aktif dan pasif yang diuji diatas, maka dapat dipilih sumber dan aksi ancaman yang pernah atau belum terjadi, tetapi kemungkinan terjadinya memiliki level "*High*", ialah sebagai berikut:

1. Ancaman yang berasal dari hacker dan cracker yang bersifat kriminal, sabotase (terorisme) atau hanya coba-coba, yaitu aktivitas hacking dan penyusupan ke sistem, kemungkinan terjadinya tinggi.
2. Ancaman yang berasal dari kegagalan perangkat lunak dan perangkat keras, yaitu gangguan listrik, kegagalan peralatan, fungsi perangkat lunak, kemungkinan terjadinya tinggi.
3. Ancaman yang berasal dari insiders, yaitu blackmail, akses ke situs yang berbahaya, system bug dan penyusupan sistem, kemungkinan terjadi tinggi.
4. Ancaman yang berasal dari kesalahan manusia, yaitu kesalahan pemasukan data, penghapusan data, kesalahan operator, kemungkinan terjadinya tinggi.
5. Ancaman yang berasal dari bencana alam, yaitu petir, kemungkinan terjadinya tinggi.

4.6 Identifikasi Kelemahan/Kerawanan (Vulnerabilities)

Vulnerability diartikan sebagai potensi kegagalan atau kelemahan yang dapat dimanfaatkan sehingga risiko terjadi, atau kelemahan sistem baik dari sisi prosedur, desain, implementasi atau kontrol internal yang dapat saja mendorong terjadinya pemanfaatan yang tidak sah atau ilegal. Dengan demikian perlu dilakukannya identifikasi terhadap kelemahan sistem yang berjalan pada perusahaan.

4.6.1 Sumber Kelemahan

Vunerability source berisi mengenai informasi kelemahan yang ada yang mungkin disebabkan oleh sumber ancaman yang telah diidentifikasi sebelumnya.

Tabel 4.22 Kelemahan (1)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
1	Industrial espionage/Pengintai	Informasi	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.
2	Kegagalan perangkat	Informasi	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.
3	Alam/Bencana Alam: Petir	Fisik: Server	Petir di lokasi tersebut, intensitasnya cukup besar, dan peralatan penangkal (antipetir dan grounding) belum mampu meredamnya.	Server terancam rusak dan terbakar, disebabkan terkena petir.
4	Kegagalan perangkat	Informasi	Perangkat DRC yang masih berada pada ruang yang sama dengan data center dan server	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.
5	Virus	Software	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.
6	Hacker, cracker, insiders	Network & Informasi	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.

Tabel 4.23 Kelemahan (2)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
7	Kegagalan perangkat: Perangkat Lunak	Software: System Backup	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.
8	Employee	Hardware & Software & Informasi	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.
9	Employee	Software & Karyawan	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.
10	Employee	Software & Karyawan	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.
11	Hacker, cracker, Employee	Software & Informasi	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.
12	Insiders	Informasi	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.

Tabel 4.24 Kelemahan (3)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
13	Vendor	Informasi	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.
14	Insiders	Informasi	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.
15	Kegagalan Perangkat	Hardware & Software & Informasi	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.
16	Insiders	Informasi	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.

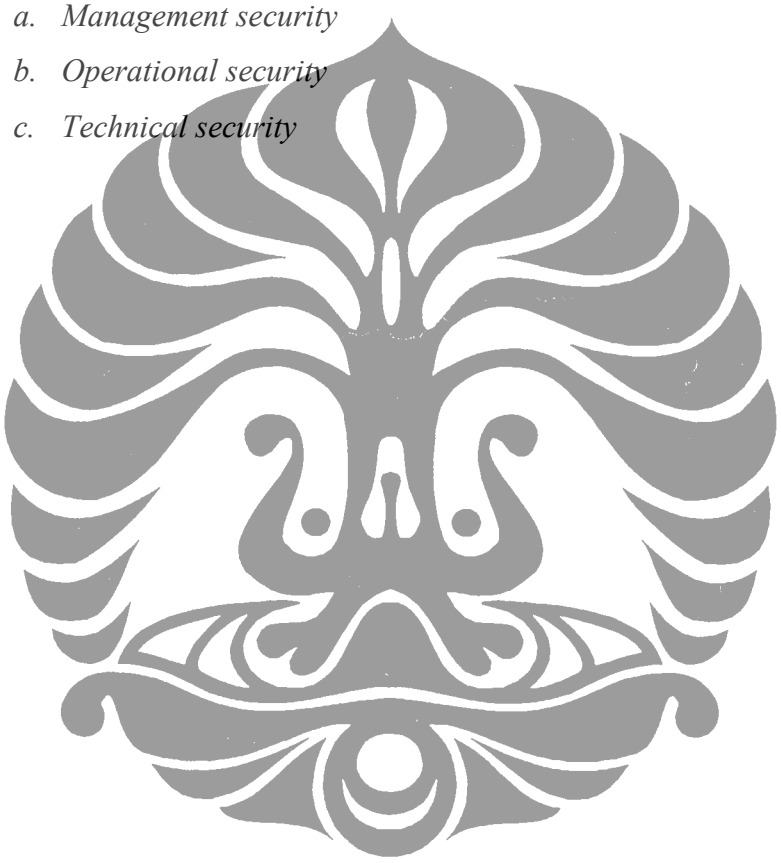
Tabel 4.25 Kelemahan (4)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
17	Hacker, cracker, insiders	Network & Informasi	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.
18	Kegagalan perangkat	Hardware & Software	Penggunaan aplikasi dan transaksi informasi yang terus bertambah, tidak terukur secara baik, 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.
19	Insiders	Karyawan & software	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.

4.6.2 Pembangunan Kebutuhan Keamanan

Security requirement checklist berisi tentang standar keamanan yang dapat digunakan untuk melakukan evaluasi dan identifikasi kelemahan keamanan aset yang dimiliki perusahaan (personil, hardware, software, dan informasi). Terdapat tiga wilayah/area evaluasi, antara lain:

a. *Management security*
b. *Operational security*
c. *Technical security*



Tabel 4.26 Hasil Pemeriksaan Kriteria Keamanan Informasi (1)

No	Security Area	Security Criteria	Telah Memenuhi		Keterangan
			Ya	Tidak	
1	**Management Security**	Terdapat penugasan mengenai tanggangjawab keamanan informasi (assignment of responsif)	√		
		Terdapat pendukung keberlangsungan bisnis (Continuity of support)	√		
		Terdapat kemampuan dalam merepons kejadian yang mendadak terjadi (incident response capability)	√		
		Secara periodik melakukan evaluasi terhadap kendali keamanan (periodic review of security controls)		√	
		Melakukan pemilihan personil yang dapat dipercaya (personnel clearance and background investigations)	√		
		Telah melakukan risk assesment		√	
		Telah melakukan pelatihan mengenai keamanan dan teknikal keamanan informasi (security and technical training)		√	
		Melakukan pembagian tugas (separation of duties)	√		
		Memiliki otorisasi pada sistem yang berjalan (system authorization and reauthorization)	√		
		Memiliki rencana keamanan sistem dan aplikasi (system and application security plan)	√		Belum tertulis

Tabel 4.27 Hasil Pemeriksanaan Kriteria Keamanan Informasi (2)

No	Security Area	Security Criteria	Telah Memenuhi		Keterangan
			Ya	Tidak	
2	**Operational Security**	Terdapat pengontrol udara dari asap, debu dan lain-lain (smoke, dust, chemicals)	√		
		Terdapat pengontrol yang dapat memastikan aliran listrik tersedia (controls to ensure the quality of the electrical power supply)	√		
		Terdapat media pengaksesan data dan penghapusan/penghancuran data (data media access and disposal)	√		
		Terdapat pengamanan pendistribusian data ke luar (External data distribution and labeling)		√	
		Terdapat fasilitas pengamanan data, seperti ruang komputer dan data center	√		
		Terdapat pengendali kelembaban ruangan (humidity control)	√		
		Terdapat pengendali suhu (temperature control)	√		
		Terdapat workstations, laptops, dan stand-alone personal computers	√		
3	**Technical Security**	Terdapat jaringan komunikasi (dial-in, system interconnection, routers)		√	
		Menggunakan teknik pengamanan data (cryptography)		√	
		Terdapat kebijakan/aturan dalam kendali akses (discretionary access control)		√	
		Terdapat identifikasi dan authentication	√		
		Terdapat pendeteksi penyusupan (intrusion detection)		√	

Tabel diatas menjelaskan bahwa:

- Pada bagian *management security*, diantar yang telah dilakukan, terdapat hal yang belum dilakukan, yaitu tidak dilakuknnya evaluasi secara periodik terhadap keamanan sistem dan kurangnya pelatihan tentang keamanan informasi kepada karyawan di divisi TI. Serta belum disusunnya sebuah rancangan keamanan informasi bagi perusahaan.
- Pada bagian *operational security*, diperoleh informasi bahwa perusahaan belum melakukan pelabelan atas informasi yang keluar dari perusahaan.
- Pada bagian *technical security*, dijelaskan bahwa perusahaan belum menerapkan teknik pengamanan data, tidak adanya kebijakan/aturan dalam kendali akses, dan perusahaan juga belum memiliki perangkat untuk mendeteksi penyusupan (*intrusion detection*)

Analisis dari data diatas, sebagai berikut:

- Tidak dilakukannya evaluasi secara periodik terhadap keamanan informasi, akan berisiko kerawanan/kelemahan sistem tidak teridentifikasi secara dini, sehingga berpotensi timbulnya ancaman dari serangan.
- Perusahaan yang belum memiliki rancangan keamanan informasi, berpotensi pembangunan TI yang dilakukan, hanya bersifat adhoc, sesuai penilaian sesaat.
- Belum dilakukannya pelabelan informasi yang keluar, akan berpotensi tidak diperhatikannya aspek perlindungan terhadap informasi tersebut, sehingga berisiko kerahasiaan informasi yang hilang.

4.7 Analisis Kontrol

Tujuan dari analisis kontrol ini ialah mampu melakukan analisis terhadap kontrol yang telah dimiliki oleh perusahaan, sebagai upaya perusahaan dalam meminimasi dan menghilangkan kemungkinan serangan yang menjadi kelemahan sistem TI yang berjalan.

4.7.1 Analisis berdasarkan Kategori Kontrol

Analisis kontrol dilakukan berdasarkan kategori kontrol yang ada, yaitu kontrol administratif, teknikal dan fisik, dengan penjelasan sebagai berikut :

- *Administrative/Management control*, yaitu kontrol keamanan yang bersifat administratif, seperti kebijakan atau prosedur, pelatihan tentang keamanan, cek latarbelakang pegawai.
- *Logical/technical control*, yaitu kontrol secara teknikal mengatur akses ke sistem dan melindungi informasi.
- *Physical/operational control*, yaitu kontrol dengan menggunakan pengamanan secara fisik, seperti fisik PC, laptop atau gedung.

Sedangkan kategori dari kontrol terdiri dari dua kategori, yaitu kategor preventive control dan detective control, dengan penjelasan sebagai berikut:

- *Preventive control*, yaitu kontrol yang digunakan untuk mencegah percobaan pelanggaran untuk mengganggu keamanan.
- *Detective control*, yaitu kontrol yang mampu memberikan peringatan, jika terjadi percobaan pelanggaran kebijakan keamanan dan kontrol pada audit trails.

Berdasarkan metode dan kategori kontrol diatas, maka dilakukan kombinasi, yang akan menjadi aspek kontrol pada observasi dan wawancara. Aspek kontrol, hasil kombinasi metode dan kategori, meliputi: *preventive – administrative, preventive – technical, preventive – physical, detective – administrative, detective – technical, detective – physical.*

Di bawah ini adalah hasil observasi dan wawancara, berdasarkan aspek kontrol diatas.

Tabel 4.28 Tabel Kombinasi Kontrol (1)

No	Control Combination	Security Criteria	Telah Memenuhi	
			Ya	Tidak
1	**Preventive-Administrative**	Adanya kebijakan dan prosedur	√	
		Adanya pemeriksaan latarbelakang sebelum karyawan bekerja	√	
		Adanya penjanjian kerja	√	
		Adanya pelabelan/kategorisasi informasi yang sensitiv		√
		Adanya penambahan pengawas (supervisor)	√	
		Pelatihan Security Awarness		√
		Pendaftaran yang mengakses SI dan Jaringan	√	
2	**Preventive-Technical**	Adanya upaya melindungi informasi dengan menggunakan protocol, encription, atau smartcard		√
		Adanya upaya melindungi informasi dengan menggunakan biometric (finger print, retina, and iris scanning)	√	
		Adanya upaya melindungi akses informasi dengan melakukan pengelolaan local and remote access control dengan menggunakan perangkat lunak	√	
		Penggunaan call-back-system		√
		Penggunaan pembatasan fungsi yang dapat diakses oleh pengguna (constrained user interface)	√	
		Penggunaan pembatasan perintah pengguna (shells)	√	
		Penggunaan pembatasan tampilan isi informasi (database views)	√	
		Rutin melakukan scanning terhadap virus komputer menggunakan perangkat lunak antivirus	√	
		Penggunaan pembatasan tombol input data (limited keypads)		√
3	**Preventive-Physical**	Terdapat penggunaan Fence, badges, multiple doors (and a man-trap), magnetic card entry systems, biometrics (for identification), guards, dogs, environmental, control systems (for humidity, temperatures, sun-light)		√
		Penempatan lokasi yang aman untuk menyimpan backup data.		√

Tabel 4.29 Tabel Kombinasi Kontrol (2)

No	Control Combination	Security Criteria	Telah Memenuhi	
			Ya	Tidak
4	**Detective-Administrative**	Organizational Policies and Procedures		√
		Background checks	√	
		Vacation Scheduling	√	
		Labeling of Sensitive Materials		√
		Increased Supervisions		√
		Security Awareness Training		√
		Behavior Awareness		√
		Sign-up Procedures	√	
		Job Rotation	√	
		Sharing Responsibilities	√	
		Review of Audit Records		√
5	**Detective-Technical**	intrusion detection systems		√
		automatically-generated violation reports from audit trail information (Log-on attempts and Log-on Entry Errors)		√
6	**Detective-Physical**	Motion Detectors		√
		Thermal Detectors		√
		Video Cameras	√	
		Metal Detectors		√
7		Security Planning		√
		Aturan tentang pemilihan password dan permintaan untuk selalu merubah password secara berkala		√
		Protection of cable	√	
		Separation of duties	√	
		Backing up files system	√	
		Kepedulian pimpinan perusahaan terhadap keamanan informasi		√

Tabel diatas menjelaskan bahwa:

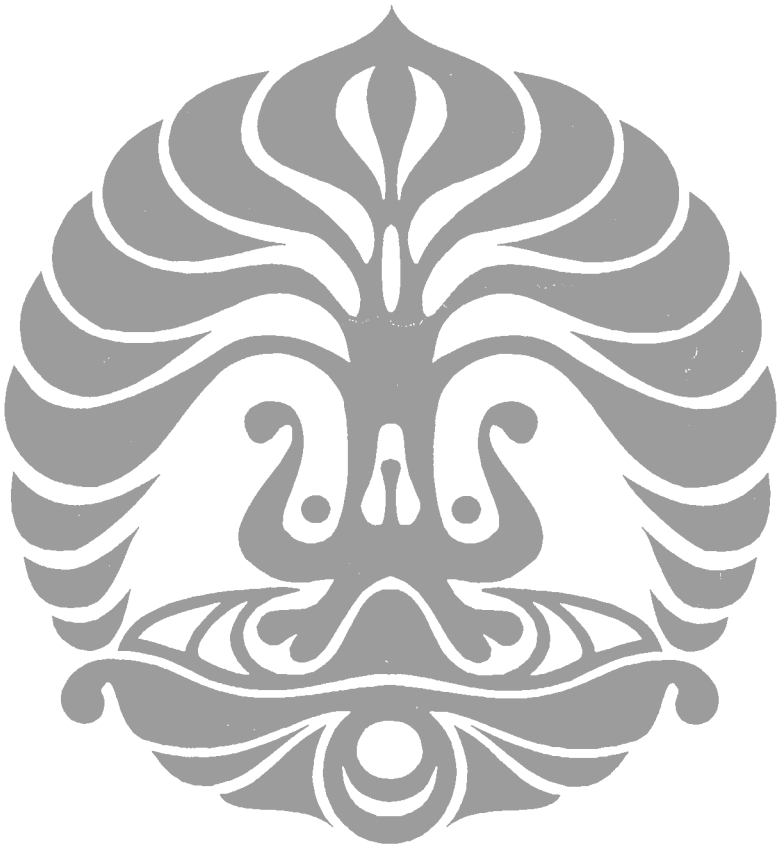
- Pada kontrol *preventive–administrative*, ditemukan bahwa tidak dilakukannya pelabelan informasi, berdasarkan klasifikasi informasinya, juga belum melakukan pelatihan untuk meningkatkan kepedulian terhadap keamanan informasi.
- Pada kontrol *preventive–technical*, dijelaskan bahwa perusahaan belum menerapkan pengamanan informasi dengan teknik enkripsi, serta belum menerapkan metode *call-back-system*, dalam memverifikasi sebuah transaksi. Dan tidak menggunakan pembatasan kontrol input data.
- Pada kontrol *preventive–physical*, bahwa belum digunakannya pengamanan dengan teknologi biometric, atau humidity temperature sebagai sistem kontrol, dan penempatan backup data yang masih berada pada satu tempat/lokasi.
- Pada kontrol *detective–administrative*, terlihat bahwa perusahaan belum memiliki kebijakan dan prosedur pengamaan informasi yang tertulis, juga belum melakukan pelabelan informasi yang sensitif, pembinaan kepedulian tentang keamanan informasi.
- Pada kontrol *detective–technical*, dinyatakan bahwa perusahaan tidak menggunakan sistem pendeteksi penyusupan (*intrusion detection system*), serta belum memiliki pelaporan upaya yang berpotensi mengganggu keamanan.
- Pada kontrol *detective–physical*, menunjukkan bahwa perusahaan belum menggunakan perangkat *motion detectors, thermal detector* atau *metal detector*.

4.7.2 Hasil Analisis Kontrol

Analisis dari hasil ceklis kombinasi kontrol diatas, diuraikan seperti di bawah ini

- Pelabelan informasi berdasarkan aspek keamanannya (*confidentiality-integrity-availability*), berguna agar terdapat perlakukan berbeda terhadap informasi dengan label sensitif. Jika belum dilakukan klasifikasi informasi, maka berisiko informasi yang senstif akan kehilangan sifat kerahasiaannya, dan dapat berakibat buruk terhadap perusahaan.
- Pelatihan dalam rangka menumbuhkan wawasan tentang kesadaran menjaga keamanan informasi sangat diperlukan, jika hal ini tidak dilakukan, maka berpotensi terjadinya gangguan yang bersumber dari kecerobohan atau kelemahan internal perusahaan.
- Belum diterapkannya metode enkripsi pada penyimpanan data dan informasi yang kritikal atau sensitif, menimbulkan risiko pencurian informasi sensitif perusahaan.
- Metode *call-back system* yang belum diterapkan, berisiko terjadinya serangan yang bersifat *social engineering*, sehingga tidak dilakukan verifikasi terhadap perintah atau transaksi penting.
- Penempatan backup yang masih berada dilokasi yang sama, yaitu pada ruang server atau data center, dapat berisiko terhentinya operasional bisnis, saat terjadi bencana pada data center, karena akan merusak data backup, yang tersimpan pada pada tempat yang sama.
- Kebijakan dan prosedur yang belum tertulis, dapat berisiko terjadinya pelanggaran yang berpotensi mengganggu keamanan informasi, karena tidak adanya panduan dan tuntunan dalam menggunakan informasi.
- Tidak digunakanya sistem pedeteksian penyusupan atau IDS, akan berpotensi terbukanya kelemahan/kerawanan sistem yang dimiliki oleh perusahaan, tanpa adanya pencegahan dan pendeteksi.

- Pelaporan atas kejadian yang berupaya atau berpotensi menggangu keamanan informasi, harus dicatat secara sistematik, untuk dianalisis dan ditindaklajuti dengan evaluasi pengamanan.
- Perangkat pendeteksian gerakan, panas temperatur atau metal yang digunakan secara tepat dalam pengamanan gudang, akan mencegah dari terjadinya pencurian barang, yang menyebabkan kehilangan kepercayaan konsumen.



4.8 Penilaian Kecenderungan (*Likelihood*) dan Analisis Dampak

Kecederungan kejadian (*likelihood*) ialah kemungkinan yang mengindikasikan peluang terjadinya resiko, yaitu adanya potensi kerawanan/kelemahan sistem. Faktor kemungkinan yang berpotensi melemahkan sistem dapat diuji dengan melihat sumber ancaman, yang dinilai dalam tingkatan tertentu. (*High, Medium, Low*)

Tabel 4.30 Tingkatan Likelihood

Kecenderungan		
Level	**Frekuensi Kejadian**	**Potensi Terjadi**
5	Sangat sering terjadi	Potensi terjadi tinggi jangka pendek
4	Lebih sering terjadi	Potensi terjadi tinggi jangka panjang
3	Cukup sering terjadi	Potensi terjadi sedang
2	Jarang terjadi	Potensi terjadi kecil
1	Hampir tidak pernah terjadi	Kemungkinan terjadi sangat kecil

Salah satu tahapan penting lainnya pada pengukuran risiko, ialah menentukan dampak yang dapat merugikan dari terjadinya ancaman terhadap kelemahan sistem. Sebelum melakukan analisis dampak, perlu diperhatikan informasi berikut:

a. Misi sistem (*system mision*)
b. Informasi yang memiliki sensitivitas.
c. Informasi yang dinilai kritikal

Adapun beberapa dampak yang mungkin ada pada perusahaan akibat dari ancaman yang disebabkan kelemahan sistem TI perusahaan, ialah :

a. Loss of integrity : hilangnya integritas sistem dan data
b. Loss of avalilability : hilangnya keberadaan atau kehandalan sistem dan data
c. Loss of confidentiality : hilangnya kerahasiaan dari informasi.

Tabel 4.31 Ukuran dari Dampak

Nilai	Dampak		
	Potensi Kerugian Finansial	**Potensi gangguan terhadap Proses Bisnis**	**Potensi penurunan Reputasi**
5	Potensi kerugian keuangan >50 juta/tahun	Terganggunya operasional proses bisnis yang terkait lebih dari satu sektor dalam mendukung tujuan organisasi	Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan dimata pelanggan/stakeholders utama, komunitas, pasar dan masyarakat secara global dan regional;
4	Potensi kerugian keuangan Rp 40 juta/tahun	Terganggunya operasional proses bisnis yang terkait dengan salah satu departemen dalam mendukung tujuan organisasi	Kerusakan reputasi yang tidak menyeluruh – hanya pelanggan atau partner bisnis (counterparties) tertentu.
3	Potensi kerugian keuangan Rp 30 juta /tahun	Terganggunya operasional proses bisnis yang terkait dengan satu divisi dalam mendukung tujuan organisasi	Kerusakan reputasi yang tidak menyeluruh – hanya di internal organisasi
2	Potensi kerugian keuangan Rp 20 juta /tahun	Terganggunya operasional proses bisnis yang terkait dengan satu Unit dalam mendukung tujuan organisasi	Kerusakan reputasi yang tidak menyeluruh – hanya di internal departemen
1	Potensi kerugian keuangan <Rp 10 juta /tahun	Tidak menyebabkan gangguan terhadap operasional proses bisnis organisasi	Tidak berpengaruh pada reputasi

Tabel 4.32 Kecenderungan dan Dampak (1)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
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.	4	4	16
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.	4	4	16
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.	4	4	16
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.	4	4	16
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.	4	4	16
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.	4	3	12
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.	4	3	12
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.	3	3	9

Tabel 4.33 Kecenderungan dan Dampak (2)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
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.	3	3	9
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.	3	3	9
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.	3	3	9
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.	3	3	9
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.	3	3	9
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.	3	3	9

Tabel 4.34 Kecenderungan dan Dampak (3)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
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.	3	3	9
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.	3	3	9
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.	3	3	9
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.	2	3	6
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.	2	3	6

4.9 Pengenalan dan Tingkat Risiko

Tujuan dari *risk determination* ialah melakukan penilaian tingkat risiko dari sistem TI yang sedang berjalan. Penentuan risiko berdasarkan ancaman dan kelemahan berdasarkan informasi sebagai berikut:

a. Kemungkinan adanya sumber ancaman (*thread-source*) yang mencoba memanfaatkan kelemahan sistem
b. Besarnya dampak yang ditimbulkan oleh berhasilnya sumber ancaman dalam memanfaatkan kelemahan sistem
c. Ketidaksiapan rancangan kontrol keamanan yang berjalan dalam mengurangi dan menghilangkan risiko tersebut.

Untuk dapat mengukur risiko tersebut, terdapar skala risiko dan risk-level matrix, yang akan menghasilkan tingkat risiko (*risk level*).

Berdasarkan penilaian kecenderungan dan dampak, pada tahapan sebelumnya, maka dilakukan pementaan level risiko, pada matrik tingkat risiko. Dimana level risiko dapat dikatakan tinggi , sedang atau rendah. Karakteristik pada setiap level, dijelaskan pada tabel di bawah ini:

Tabel 4.35 Risk Scale and Necessary Actions

Risk Level	Ranking	Risk Description and Necessary Actions
Extreme	20 - 25	Level Risiko tertinggi
High	12- 16	Jika terdapat gangguan, mungkin saja sistem yang ada masih tetap berjalan, tetapi rencana tindakan perbaikan harus segera dilakukan.
Medium	6 -10	Jika terdapat gangguan, rencana tindakan perbaikan dapat dilakukan pada waktu memungkinkan
Low	0 - 5	Jika terdapat gangguan, rencana tindakan perbaikan perlu dilakukan, atau perusahaan dapat memutuskan untuk menerima risiko tersebut.

Tabel 4.36 Identifikasi Tingkat Risiko (1)

No	Risk	Likelihood Level	Impact Level	Ranking	Risk Level
1	Risiko kehilangan keamanan informasi (confidentiality, integrity, avalailability), jika informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka.	4	4	16	H
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.	4	4	16	H
3	Petir di lokasi tersebut, intensitasnya cukup besar, sedang penangkalnya belum mampu meredamnya, disebabkan tidak memiliki groundded yang baik, sehingga berpotensi merusak dan membakar server dan perangkat jaringan.	4	4	16	H
4	Risiko hilangnya data master dan backup berpotensi terjadi, jika ruang DRC berada berada pada ruang yang sama dengan ruang data center atau server yang saat mengalami bencana	4	4	16	H
5	Risiko penggunaan sistem operasi yang rentan dengan gangguan virus, tanpa didukung oleh perangkat antivirus yang cukup handal, berpotensi menimbulkan kerusakan file, dan kehilangan file data.	4	4	16	H
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.	4	3	12	H
7	File system backup gagal saat direstore, maka berpotensi jika terjadi kehilangan data pada sistem utama, maka hasil backup tidak dapat direstore, sehingga harus men-entry ulang secara berdasarkan form manual.	4	3	12	H
8	Pegawai yang telah menguasai bisnis proses dan pengelolaan teknologinya, masih berstatus pegawai kontrak, sehingga berpotensi pegawai IT dapat keluar kapan pun dari perusahaan, divisi IT kekurangan pegawai terlatih.	3	3	9	M
9	Risiko karyawan tidak mampu menguasai secara cepat teknologi yang digunakan perusahaan, karena tidak memiliki keterampilan dan pengalaman yang cukup di bidang TI sehingga proses monitoring dan pemeliharaaan sistem menjadi lambat dan terhambat.	3	3	9	M

Tabel 4.37 Identifikasi Tingkat Risiko (2)

No	Risk	Likelihood Level	Impact Level	Ranking	Risk Level
10	Risiko layanan bongkar muat yang membutuhkan waktu yang lama, sehingga akan merusak citra perusahaan, akibat kesalahan entry oleh operator, informasi no petikemas dan lokasi petikemas terjadi	3	3	9	M
11	Risiko jika perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, menyebabkan kelemahan tersebut diketahui orang, yang akan mengganggu keamanan informasi. Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi.	3	3	9	M
12	Risiko terganggunya keamanan informasi, jika perusahaan memiliki karyawan baru tidak akan pernah mengetahui tentang kebijakan perusahaan dalam pengamanan informasinya, karena kebijakan yang tidak tertulis dan kurangnya sosialisasi.	3	3	9	M
13	Risiko integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai, jika aplikasi yang dibangun dengan platform DBMS yang berbeda.	3	3	9	M
14	Risiko kehilangan keamanan informasi (confidentiality, integrity, avalailability), jika terjadi modifikasi informasi dan pencurian informasi melalui komputer yang tidak menerapkan keamaan desktop, saat pemiliknya tidak berada ditempat.	3	3	9	M
15	Risiko kerusakan perangkat komputer/server karena suhu ruangan yang tinggi, jika pemeliharaan terhadap perangkat pengatur suhu ruangan server/data center.	3	3	9	M
16	Risiko pencurian informasi oleh insiders, jika belum mengimpelentasikan enkripsi pada penyimpanan informasi rahasia.	3	3	9	M
17	Risiko masuknya gangguan keamanan pada komputer personal cukup tinggi, karena tidak diaktifkannya firewall, jika tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.	3	3	9	M
18	Resiko menurunnya kecepataan server dan aplikasi karena beban yang tinggi, sebab tidak terukurnya kinerja dan beban sistem secara tepat, jika belum diterapkannya pengujian keamaanan sistem yang berjalan.	2	3	6	M
19	Banyaknya operator, yang Operator dengan jumlah yang cukup banyak, dan mayoritas berstatus kontrak harian, perlu menjadi perhatian, karena sangat rentan dengan gangguan internal (insider), dan rentan dengan penyalahgunaan.	2	2	4	L

Berdasarkan tabel diatas, mengenai risiko, kecenderungan, dan dampaknya, dapat digambarkan dengan matriks di bawah ini.

Kecenderungan

5	Low	Medium	High	Extreme	Extreme
4	Low	Medium	High	High	Extreme
3	Low	Medium	Medium	High	High
2	Low	Low	Medium	Medium	Medium
1	Low	Low	Low	Low	Low
	1	2	3	4	5

Dampak

Gambar 4.3 Matriks Tingkat Risiko

Dari gambar matriks tingkat risiko diatas, maka dapat dijelaskan bahwa:

- Perusahaan mencapai *high*, untuk beberapa risiko, hal ini akan harus menjadi prioritas utama dalam perancangan keamanan informasi.
- Sedangkan level *medium* dan *low*, dpat menjadi bagian dari perancangan keamanan informasi

Tingkat risiko juga dapat diuraikan secara kuantitatif, untuk risiko petir di lokasi tersebut, intensitasnya cukup besar, sedang penangkalnya belum mampu meredamnya, disebabkan tidak memiliki grounding yang baik, sehingga berpotensi merusak dan membakar server, switch dan access point, seperti di bawah ini:

Tabel 4.38 Analisis Kuantitatif pada Risiko akibat Gangguan Petir

Risiko	Aset	Spec	Nilai Aset ($)	Nilai Aset (Rp)	EF	SLE	ARO	ALE
Petir di lokasi tersebut, intensitasnya cukup besar, sedang penangkalnya belum mampu meredamnya, disebabkan tidak memiliki groundded yang baik, sehingga berpotensi merusak dan membakar server.	Server		5,500	66,000,000	100.00%	66,000,000	0.4	26,400,000
	Switch	3COM 3C17100	1,600	19,200,000	100.00%	19,200,000	0.4	7,680,000
	Access Point Wireless	3COM 3CRWEA SYA73	1,500	18,000,000	100.00%	18,000,000	0.4	7,200,000
	Biaya per tahun atas risiko tersebut							41,280,000

Dari perhitungan diatas, maka setiap tahunnya diperkirakan perusahaan akan mengeluarkan biaya atas risiko tersebut, sebesar Rp. 41.280.000,- per tahun. Berdasarkan analisis risiko secara kuantitatif, pada risiko kerusakan server dan perangkat jaringan, akibat petir, yang sering terjadi. Analisis risko secara kuantitatif, sulit dilakukan terhadap risiko yang berdampak secara intangible dan selanjutnya tangible, contohnya risko yang berdampak pada tersebarnya informasi rahasia miliki perusahaan di publik. Hal ini berdampak pada kepercayaan konsumen pada perusahaan (intangible), dan selanjutnya akan menurunkan pendapatan perusahaan, karena konsumen yang mulai berkurang, dan beralih ke perusahaan pesaing. Risiko tersebut secara kuantitatif dapat dinilai dengan ukuran kecenderungan dan dampak secara kualitatif, yang sulit dan perlu metode dalam menilai risiko tersebut secara kuantitatif.

4.10 Rekomendasi Kontrol

Pada tahap *control recommendations* ini, dilakukan menyampaikan beberapa rekomendasi kontrol yang dapat diharapkan mampu meredakan atau mengurangi risiko yang ada. Adapun dasar dari rekomendasi sebuah kontrol ialah kemampuan kontrol tersebut dalam menurunkan risiko, berdasarkan penjelasan literatur dan *best practice*. Penilaian terhadap evaluasi dan analisis cost-benefit dan cost-effectiveness dari setiap kontrol akan dilakukan pada tahap risk mitigation, sehingga akan diperoleh penilaian yang tidak hanya didasarkan pada literatur atau *best practice*, tetapi akan dianalisis kesesuaian dan kemampuan dalam menurunkan risiko.

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

Adapun rekomendasi yang dihasilkan dari penaksiran risiko atau analsisi risiko diatas, 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 4.39 Recomendasi kontrol (1)

No	Risk	Ranking	Risk Level	Recommended Control
1	Risiko kehilangan keamanan informasi (confidentiality, integrity, avalailability), 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 groundded 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 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 file data.	16	H	**Preventive**:Pelatihan Security Awarness (ADM), scanning terhadap virus (TECH) **Detective**: Pelatihan Security Awarness (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), Intrusion Detection Systems (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 men-entry ulang secara berdasarkan form manual.	12	H	**Preventive**:Kebijakan dan prosedur (ADM), Penyimpanan Backup di tempat aman (PHY) **Detective**: Sharing Responsibilities (ADM)
8	Pegawai yang telah menguasai bisnis proses dan pengelolaan teknologinya, masih berstatus pegawai kontrak, sehingga berpotensi pegawai IT dapat keluar kapan pun dari perusahaan, divisi IT kekurangan pegawai terlatih.	9	M	**Preventive**:Perjanjian kerja (ADM) **Detective**: Penilaian Latar Belakang(ADM)

Tabel 4.40 Recomendasi kontrol (2)

No	Risk	Ranking	Risk Level	Recommended Control
9	Risiko karyawan tidak mampu menguasai secara cepat teknologi yang digunakan perusahaan, karena tidak memiliki keterampilan dan pengalaman yang cukup di bidang TI, agar dapat melakukan monitoring dan pengembangan TI milik perusahaan.	9	M	**Preventive**:Penilaian Latar Belakang(ADM)
10	Resiko layanan bongkar muat yang membutuhkan waktu yang lama, sehingga akan merusak citra perusahaan, akibat kesalahan entry oleh operator, informasi no petikemas dan lokasi petikemas terjadi	9	M	**Preventive**:Kebijakan dan prosedur (ADM), Penggunaan call-back-system (TECH) **Detective**: Kebijakan dan prosedur (ADM), Audit trail information (TECH)
11	Risiko jika perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, menyebabkan kelemahan tersebut diketahui orang, yang akan mengganggu keamanan informasi. Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi	9	M	**Preventive**:Pelatihan Security Awarness (ADM), Penggunaan call-back-system (TECH) **Detective**: Kebijakan dan prosedur (ADM),intrusion detection systems (TECH)
12	Risiko terganggunya keamanan informasi, jika perusahaan memiliki karyawan baru tidak akan pernah mengetahui tentang kebijakan perusahaan dalam pengamanan informasinya, karena kebijakan yang tidak tertulis dan kurangnya sosialisasi.	9	M	**Preventive**:Pelatihan Security Awarness (ADM), Pembatasan fungsi dan Informasi (TECH) **Detective**: Pelabelan Informasi sensitif (ADM)
13	Risiko integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai, jika aplikasi yang dibangun dengan platform DBMS yang berbeda.	9	M	**Preventive**:Kebijakan dan prosedur (ADM) **Detective**: Kebijakan dan prosedur (ADM)
14	Risiko kehilangan keamanan informasi (confidentiality, integrity, avalailability), jika terjadi modifikasi informasi dan pencurian informasi melalui komputer yang terbuka, saat pemiliknya tidak berada ditempat.	9	M	**Preventive**:Kebijakan dan prosedur (ADM), Pembatasan fungsi dan Informasi (TECH) **Detective**: Kebijakan dan prosedur (ADM), Intrusion Detection Systems (TECH)

Tabel 4.41 Recomendasi kontrol (3)

No	Risk	Ranking	Risk Level	Recommended Control
15	Risiko kerusakan perangkat komputer/server karena suhu ruangan yang tinggi, jika pemeliharaan terhadap perangkat pengatur suhu ruangan server/data center.	9	M	**Preventive**:Kebijakan dan prosedur (ADM)
				Detective: Kebijakan dan prosedur (ADM)
16	Risiko pencurian informasi oleh insiders, jika belum mengimpelentasikan enkripsi pada penyimpanan informasi rahasia.	9	M	**Preventive**:Kebijakan dan prosedur (ADM), Enkripsi (TECH)
				Detective: Pelabelan Informasi sensitif (ADM), violation reports (TECH)
17	Risiko masuknya gangguan keamanan pada komputer personal cukup tinggi, karena tidak diaktifkannya firewall, jika tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.	9	M	**Preventive**:Kebijakan dan prosedur (ADM)
				Detective: Kebijakan dan prosedur (ADM), violation reports (TECH)
12	Resiko menurunnya kecepataan server dan aplikasi karena beban yang tinggi, sebab tidak terukurnya kinerja dan beban sistem secara tepat, jika belum diterapkannya pengujian keamaanan sistem yang berjalan.	6	M	**Preventive**:Kebijakan dan prosedur (ADM)
				Detective: Kebijakan dan prosedur (ADM)
17	Banyaknya operator, yang Operator dengan jumlah yang cukup banyak, dan mayoritas berstatus kontrak harian, perlu menjadi perhatian, karena sangat rentan dengan gangguan internal (insider), dan rentan dengan penyalahgunaan..	4	L	**Preventive**:Kebijakan dan prosedur (ADM), Pembatasan fungsi dan Informasi (TECH)
				Detective: Increased Supervisions(ADM), violation reports (TECH)

Tabel rekomendasi kontrol akan menjadi hasil dari tahap penilaian risiko, yang selanjutnya akan menjadi input bagi tahap risk mitigation, akan melakukan evaluasi, analisis cost-benefit, cost effectiveness terhadap kontrol keamanan yang direkomendasikan, dan pada akhirnya akan dipilih. Pembahasan tentang tahap proses mitigation, akan dijelaskan pada bagian selanjutnya.