BAB 1 PENDAHULUAN

1.1 Latar Belakang

PT Matahari Department Store merupakan perusahaan ritel di Indonesia. PT Matahari Dept Store memiliki visi baru yaitu semua orang Indonesia dapat tampil menarik dan nyaman, terkait hal tersebut maka perlu dilakukan pembenahan-pembenahan seiring dengan kompleksitas proses yang dikelola juga semakin meningkat. Selain itu, pemenuhan kebutuhan informasi bagi seluruh civitas perusahaan juga harus memadai, hal ini untuk menunjang aktivitas di PT Matahari Department Store. Oleh karena itu, perusahaan ini memiliki sebuah unit yang bernama Tim EDP.

Tim EDP (*Ending Data Proses*) adalah sebuah unit pelaksana teknis yang memberikan support terhadap teknologi informasi bagi semua fungsi di perusahaan dengan mengembangkan sistem informasi terpadu sesuai kebutuhan perusahaan beserta investasi infrastruktur yang diperlukan untuk menunjang bisnis perusahaan. Alphapos merupakan aplikasi penjualan serta pelaporan keuangan yang digunakan oleh staff, supervisor (*first line Manager*), asisten *store Manager*(*middle Manager*) serta*store Manager*(*top level*) untuk semua fungsi di PT Matahari Dept Store. Alphapos memproses transaksi-transaksi yang terjadi di *front office* dan *back office*, meliputi penjualan dan pembelian. Transaksi tersebut akan diproses menjadi laporan-laporan baik berupa statistik ataupun tabel. Oleh sebab itu, kehadiran Alphapos dinilai sangat penting dalam penyampaian informasi ke seluruh *civitas* perusahaan, hal ini membuat sistem penjualan Alphapos harus berjalan optimal dan konsisten.

Namun berbagai kemungkinan ancaman dan risiko yang muncul dapat mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Kemungkinan ancaman dan risiko tersebut dapat berasal dari berbagai elemen, salah satunya dapat berasal dari Teknologi dan Infrastruktur sistem.

Beberapa penelitian menunjukan bahwa teknologi informasi beserta asetnya rentan terhadap risiko kerusakan fisik dan kerusakan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (*natural disaster*), pencurian (*thief*), kebakaran (*fires*), lonjakan listrik (*power surge*) dan perusakan (*vandalism*). Risiko kerusakan logik mengacu pada akses yang tidak sah (*unauthorized access*), kerusakan secara sengaja maupun tidak sengaja pada teknologi informasi dan aset informasi yang terkandung didalamnya. Untuk itu diperlukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi.

Pada bulan November tahun 2009, *International Organization for Standaritation* (ISO) mengeluarkan *framework* standar untuk mengelola risiko yaitu ISO 31000:2009 dengan judul "*Risk Management-Principles and Guidelines*

on Implementation". Standar ini dikeluarkan untuk membantu perusahaan dalam mengelola risiko. Karena sifatnya yang generik, *framework* ini dapat diaplikasikan di berbagai jenis perusahaan, grup atau individu. ISO 31000:2009 menyediakan panduan dalam mendesain, implementasi dan memelihara proses pengelolaan risiko di dalam sebuah organisasi.

Sebelumnya perusahaan menggunakan *framework* ASEAN *Corporate Governance Scorecard* (ACGS) yang memiliki fokus pada bidang bisnis secara umum. Namun, kelemahan dari *framework* ini adalah tidak adanya fokus pada risiko bidang teknologi informasi. Sehingga hingga saat ini untuk dokumentasi risiko teknologi informasi belum ada terutama mengenai sistem penjualan Alphapos.

Berangkat dari permasalahan di atas, maka peneliti mencoba mengimplementasikan suatu analisis manajemen risiko menggunakan ISO 31000 yang dapat digunakan untuk mengelola risiko secara keseluruhan pada suatu area kegiatan sehingga perusahaan dapat melakukan pencegahan, penanganan, serta perbaikan kedepannya.

Penelitian sebelumnya yang dilakukan oleh Anthon R. Tampubolon dan Suhardi (2015) dengan menggunakan *framework* manajemen risiko ISO 31000:2009, dapat disimpulkan bahwa manajemen risiko penting dilakukan untuk menjaga tercapainya tujuan perusahaan. Untuk *framework* ISO 31000:2009 dapat diimplementasikan dalam manajemen risiko bidang TI pada sebuah industry perbankan. Dengan perlakuan risiko yang tidak tepat dapat meningkatkan *likelihood* atau kriteria kemungkinan dari sebuah *risk event*. Dalam penelitian ini juga menyimpulkan bahwa mitigasi adalah [erlakuan risiko yang tepat dalam mencegah terulangnya pembobolan ATM di BCA.

Sedangkan penelitian sebelumnya yang dilakukan oleh Nazruddin Safaat H (2011) dengan manajemen risiko terkait risiko TI khususnya risiko kegagalan sistem infrastruktur akibat gangguan alam dapat disimpulkan bahwa penggunaan *framework* manajemen risiko TI dengan ISO 31000:2009 dapat membantu proses pengambilan keputusan berdasarkan hasil *risk assessment* yang dilakukan. Sumber risiko yang bisa berdampak langsung terhadap tujuan dan startegis perusahaan dianjurkan harus selalu di *monitor* dan *review,* karena perubahan masa akan memerlukan teknik penanganan yang lebih efektif.

Berdasarkan hasil analisis, didapatkan gambaran terdokumentasi mengenai kemungkinan ancaman dan risiko yang muncul pada teknologi dan infrastruktur sistem penjualan Alphapos serta bagaimana pencegahan, penanganan, dan perbaikan yang dapat dilakukan institusi untuk mengelola kemungkinan ancaman dan risiko tersebut. Sehingga dalam penelitian ini dibutuhkan identifikasi risiko teknologi informasi pada sistem penjualan Alphapos, tingkat prioritas untuk risiko teknologi informasi pada sistem penjualan Alphapos, serta mitigasi yang tepat untuk risiko teknologi informasi pada sistem penjualan Alphapos

1.2 Rumusan Masalah

Dari uraian latar belakang terdapat beberapa rumusan masalah yang digunakan pada penelitian ini, sebagai berikut:

1. Bagaimana identifikasi risiko teknologi informasi terhadap sistem penjualan Alphapos menggunakan ISO 31000?
2. Bagaimana tingkat prioritas risiko teknologi informasi sistem penjualan Alphapos menggunakan ISO 31000?
3. Bagaimana mitigasi risiko teknologi informasi sistem penjualan Alphapos menggunakan ISO 31000?

1.3 Tujuan

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Melakukan tahapan dan proses analisis risiko teknologi informasi berbasis manajemen risiko sesuai dengan standar dan kerangka kerja ISO 31000.
2. Mengetahui tingkat prioritas risiko teknologi informasi sistem penjualan Alphapos menggunakan ISO 31000.
3. Mengetahui mitigasi risiko teknologi informasi sistem penjualan Alphapos menggunakan ISO 31000.

1.4 Manfaat

Beberapa manfaat yang ingin dicapai pada penelitian ini adalah sebagai berikut:

1. Bagi perusahaan
   Hasil penelitian yang diperoleh dapat dijadikan masukan serta sebagai sumbangan pemikiran berupa saran dalam manajemen risiko yang sesuai dengan sistem penjualan yang digunakan oleh perusahaan.
2. Bagi pihak lain
   Hasil penelitian yang diperoleh dapat menambah pengetahuan dan wawasan serta bagaimana penerapan manajemen risiko dalam suatu perusahaan dari teori yang ada serta sebagai bahan materi dan sumber informasi.

1.5 Batasan Masalah

Batasan masalah yang digunakan pada penelitian ini adalah sebagai berikut:

1. Identifikasi risiko teknologi informasi pada sistem penjualan Alphapos menggunakan ISO 31000.
2. Penilaian risiko hanya difokuskan pada teknologi dan infrastruktur sistem penjualan Alphapos untuk mengurangi atau meniadakan dampak negatif yang timbul dari kemungkinan risiko yang muncul.

3. Responden atau narasumber merupakan staff IT atau pihak-pihak yang terlibat langsung dengan sistem dan permasalahan pengolahan pada sistem penjualan Alphapos.
4. Penelitian bersifat *descriptive.*
5. Pada penelitian ini tidak melibatkan proses *monitoring* dan *review*.

1.6 Sistematika Pembahasan

Penelitian ini disusun secara sistematis berdasarkan tata tulis penelitian yang telah ditetapkan oleh Program Studi Strata Satu Sistem Infomasi Fakultas Ilmu Komputer Universitas Brawijaya Malang dengan urutan penyajian sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisi gambaran umum tentang penelitian yang akan dilaksanakan. Bagian-bagian yang merupakan penjabaran dalam bab ini adalah latar belakang masalah, tujuan dan manfaat pembuatan skripsi, permasalahan, batasan masalah, dan sistematika penyusunan skripsi.

BAB 2 LANDASAN KEPUSTAKAAN

Bab ini membahas tentang penelitian sejenis yang sudah dilakukan oleh penulis lain, serta sebagai referensi dalam menyusun penelitian. Serta sebagai dasar dalam melakukan penelitian pada bidang teknologi informasi dan teori-teori tentang kerangka kerja manajemen risiko teknologi informasi menggunakan ISO 31000.

BAB 3 METODOLOGI PENELITAN

Bab ini menjelaskan metode yang dilaksanakan dalam penelitian yang dimulai dari metode dan teknik pengumpulan data yang digunakan.

BAB 4 PENGUMPULAN DATA

Bab ini menjelaskan mengenai proses pengumpulan data untuk memenuhi kebutuhan penelitian ini, dimana pengumpulan data dilakukan di PT Matahari Department Store.

BAB 5 PEMBAHASAN

Bab ini menjelaskan hasil dari analisis data lapangan yang telah dilaksanakan dengan metode penelitian yang telah diuraikan pada bab-bab sebelumnya. Pembahasan dimulai dari penerapan kerangka kerja manajemen sistem informasi penjualan, deskripsi kerangka kerja dan penerapannya di PT Matahari Department Store dan faktor-faktor apa yang mempengaruhi pelaksanaan manajemen risiko sistem informasi penjualan.

repository.ub.ac.id

BAB 6 PENUTUP

Bab ini menjelaskan mengenai kesimpulan yang diperoleh peneliti selama melaksanakan penelitian dan menganalisis data. Kesimpulan merupakan hasil dari jawaban perumusan masalah yang dikaji dalam penelitian. Saran diberikan kepada penelitian yang telah dilaksanakan tetapi tidak bisa menjawab perumusan masalah yang dikemukakan. Saran diberikan sebagai hasil rekomendasi terhadap penelitian yang akan dilaksanakan mendatang yang merupakan hasil analisis risiko bagi PT Matahari Department Store.

UNIVERSITAS BRAWIJAYA

UNIVERSITAS BRAWIJAYA

BAB 2 LANDASAN KEPUSTAKAAN

2.1. Kajian Pustaka

Terdapat beberapa penelitian yang digunakan peneliti untuk membandingkan metode yang akan digunakan. Pada penelitian ini, penulis menggunakan kerangka kerja ISO 31000 sebagai *framework* untuk manajemen risiko. Terdapat beberapa jurnal penelitian yang digunakan sebagai acuan dalam penelitian ini.

Penelitian pertama dengan judul "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010" yang ditulis oleh Tampubolon & Suhardi (2011) menjelaskan bahwa Teknologi Informasi (TI) telah menjadi suatu kebutuhan hampir disemua bidang usaha. Baik itu di bidang perbankan, pemerintahan, maupun di bidang pendidikan. Di bidang perbankan retail misalnya, TI memberikan banyak pilihan bagi nasabah untuk memudahkan proses transaksi, transaksi dapat dilakukan dimana saja dan kapan saja dengan menggunakan layanan ATM (*Automatic Teller Machine*), EDC (*Electronic Data Capture*), *m-banking (mobile Banking)*, maupun *i-banking(Internet Banking)*. Layanan-layanan TI ini bahkan telah mengubah paradigma nasabah dalam bertransaksi.

Namun kemajuan TI ini tidak terhindar dari risiko yang dapat membuat tidak terwujudnya tujuan dari penggunaan TI tersebut. Pembobolan ATM adalah salah satu risiko yang harus dihadapi oleh pihak bank maupun pihak nasabah. Pihak Bank dapat mengalami ketidakpercayaan nasabah yang berdampak pada penurunan reputasi dimata nasabahnya,sedangkan pihak nasabah mengalami kerugian akibatkehilangan dana di rekeningnya.

Risiko-risiko tersebut dapat dihadapi dengan membuat suatu tata kelola (Manajemen Risiko) yang baik sehingga dapat memberikan pertimbangan kepada perusahaan secara terstruktur dengan memperhatikan segala bentuk ketidakpastian dalam pengambilan keputusan dan tindakan yang harus diambil guna menangani risiko tersebut. Tata kelola inilah yang disebut dengan *Enterprise Risk Management* (ERM).

Hasil penelitian tersebut dapat diambil kesimpulan sebagai berikut:

1. Manajemen Risiko penting dilakukan untuk menjaga tercapainya Tujuan dari Perusahaan.
2. ISO 31000:2009 dapat diimplementasikan dalam Manajemen Risiko bidang TI pada sebuah industri perbankan.
3. Perlakuan Risiko yang tidak tepat dapat meningkatkan *likelihood* atau Kriteria Kemungkinan dari sebuah *Risk Event*.
4. Mitigasi adalah perlakuan risiko yang tepat dalam mencegah terulangnya pembobolan ATM di BCA.

Penelitian selanjutnya dengan judul "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 (Studi Kasus : Sistem Infrastruktur TI Telkom Indonesia)" oleh Safaat (2011) menjelaskan bahwa banyaknya bencana alam yang terjadi di Indonesia sering mengakibatkan tidak berfungsinya sistem infrastruktur TI PT. Telkom Indonesia sehingga pelanggan tidak bisa menggunakan layanan dari Telkom. Sistem Infrastruktur TI merupakan aset penting maka harus dikelola secara efektif untuk memaksimalkan efektivitas penggunaannya dan agar risiko terkait dari teknologi yang diimplementasikan dapat dimitigasi.Manajemen risiko dapat memberikan pertimbangan secara terstruktur dengan memperhatikan segala bentuk ketidakpastian dalam pengambilan keputusan dan tindakan yang harus diambil guna menangani berbagai risiko tersebut. Paper ini menyajikan sebuah studi kasus tentang permasalahan terkait TI yang terjadi pada perusahaandi sektorindustrilayanan telekomunikasi, analisis dilakukan dengan menggunakan framework ISO 31000:2009. Framework ini mempertimbangkan risiko TI sebagai bagianintegral dari kerangka risiko perusahaan.

Hasil penelitian tersebut dapat diambil kesimpulan sebagai berikut:

1. Penggunaan *Framework* manajemen risiko TI dengan ISO 31000:2009 ini dapat membantu proses pengambilan keputusan berdasarkan hasil *risk assessment* yang dilakukan.
2. Sumber risiko yang bisa berdampak langsung terhadap tujuan dan stategis perusahaan dianjurkan harus selalu di *monitor* dan *review*, karena perubahan masa akan memerlukan teknik penanganan yang lebih efektif.

Penelitian selanjutnya yang berjudul "Evaluasi Pengendalian Aplikasi Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA)" dilakukan oleh Sari, Papilaya, & Manuputty (2017) menyimpulkan bahwa Pengendalian terhadap aplikasi dilakukan untuk meningkatkan kinerja aplikasi itu sendiri dan untuk meminimalisir risiko yang ditimbulkan. Dengan merancang uji pengendalian secara detail akan membuat organisasi mendapatkan informasi secara lengkap mengenai kelebihan dan kelemahan aplikasinya. Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA) merupakan aplikasi transaksi keuangan yang terus mengalami perkembangan ke versi yang lebih baru. Oleh sebab itu dirasa perlu untuk melakukan evaluasi pengendalian aplikasi guna mengetahui keandalan aplikasi SIKASA, dan untuk meminimalisir risiko yang ada. Metode penelitian yang dipakai menggunakan pendekatan deskriptif kualitatif dengan mengumpulkan data melalui serangkaian wawancara dan observasi. Konsep '*audit through the computer*' juga dipilih untuk melakukan pengujian pada prosedur *input, process*, dan *output* data. Hasil penelitian ini diperoleh kelebihan, kelemahan, risiko dan rekomendasi atas evaluasi pengendalian aplikasi. Guna mendukung rekomendasi yang diberikan peneliti adalah baik dan efektif untuk diterapkan, dibuktikan dengan melakukan perhitungan nilai pada setiap kategori

pengendalian menggunakan matriks. Dibuktikan pula dengan mencari nilai rata-rata pengendalian secara keseluruhan, dimana pada penelitian ini didapatkan nilai 4,7 poin (positif).

2.2. Profil Perusahaan

2.2.1. PT. Matahari Department Store Tbk – Malang Town Square

PT Matahari Department Store Tbk ("Matahari" atau "Perseroan") memiliki sejarah yang panjang dalam dunia ritel Indonesia. Memulai perjalanan pada tanggal 24 Oktober 1958 dengan membuka gerai pertamanya berupa toko fashion anak-anak di daerah Pasar Baru Jakarta, Matahari melangkah maju dengan membuka department store modern pertama di Indonesia pada tahun 1972. Sejak itu Matahari telah menjadikan dirinya sebagai merek asli nasional. Sampai saat ini mengoperasikan 156 gerai dengan luas ruang usaha lebih dari satu juta meter persegi yang tersebar di 73 kota di seluruh Indonesia, dengan luas ruang lebih dari satu juta meter persegi dan telah mengembangkan kehadirannya dalam dunia online melalui MatahariStore.com.

Dengan perjalanan usaha yang telah dibangun selama 59 tahun, Matahari senantiasa menyediakan pilihan fashion dengan trend terkini untuk kategori pakaian dan mode, serta produk-produk kecantikan dan barang-barang keperluan rumah tangga lainnya yang ditampilkan dalam gerai modern serta MatahariStore.com. Matahari sangat bangga atas dukungannya terhadap perekonomian Indonesia dengan mempekerjakan lebih dari 40.000 karyawan dan ber-partner dengan sekitar 850 pemasok lokal serta pemasok internasional.

PT Matahari Department Store Tbk cabang Malang Town Square telah menggunakan sistem penjualan Alphapos semenjak tahun 2005. Sistem penjualan Alphapos sendiri berfungsi sebagai sistem pemrosesan transaksi yang digunakan untuk menghimpun, menyimpan, dan memproses data transaksi serta kadangkala mengendalikan keputusan yang merupakan bagian dari transaksi. Hingga saat ini Alphapos merupakan bagian penting dalam suatu gerai Matahari Department Store, karena Alphapos selain sebagai penyedia data juga sebagai pemroses data yang diperlukan oleh gerai.

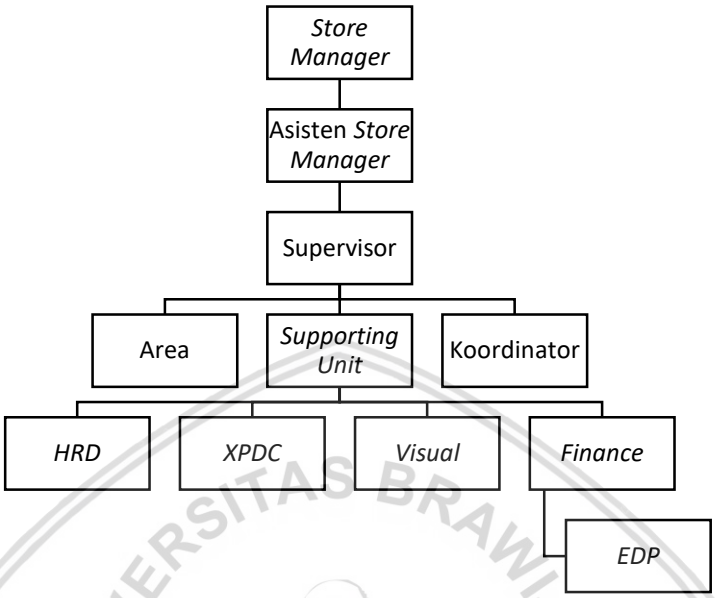
2.2.2. Visi dan Misi Matahari

Berikut merupakan visi dan misi dari PT Matahari Department Store:

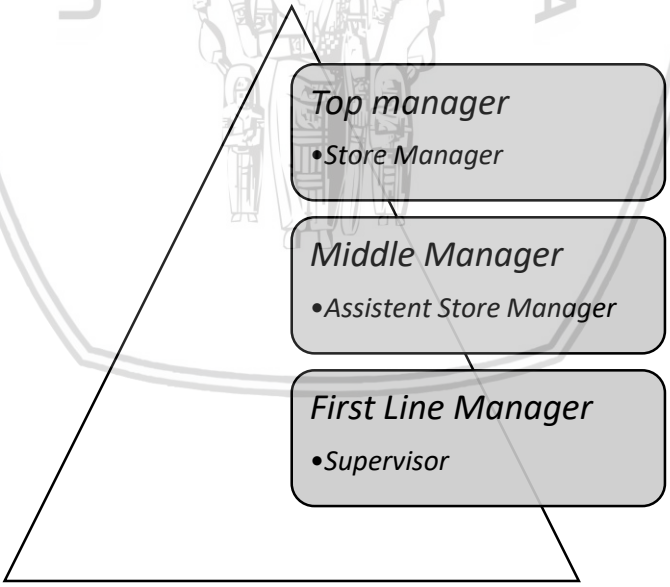
a. Visi
   Menjadi peritel pilihan utama Indonesia
b. Misi
   Secara konsisten menyediakan beragam produk fashion yang tepat serta layanan terbaik untuk meningkatkan kualitas hidup konsumen.

2.2.3.Struktur Organisasi

2.2.3.1. Bagan Struktur Organisasi



Gambar 2. 1 Struktur organisasi Matahari Department Store Malang Town Square



Gambar 2. 2 Piramida *Manager* pada Matahari Dept Store Malang Town Square

2.2.3.2 Deskripsi Pekerjaan

Untuk pembagian tugas dan wewenang dari bagian adalah sebagai berikut:

1. *Store Manager*
   Memimpin suatu sub fungsi kerja (*department*), yang dituntut untuk memiliki perspektif menyeluruh dalam bisnis, perencanaan jangka

pendek serta mengembangkan konsep kerja, kebijakan-kebijakan dalam area kerjanya

2. Asisten *Store Manager*
   Dalam level ini dituntut untuk supervisi tim yang lebih besar dengan kemampuan kepemimpinan, *problem solving* serta komunikasi yang tinggi dengan kemampuan teknis yang tinggi
3. *Supervisor*
   Bertanggung jawab terhadap tugas keseharian operasional secara tim maupun individu yang memerlukan kemampuan yang spesifik
4. *Staff*
   Bertanggung jawab terhadap eksekusi tugas keseharian operasional secara individual dengan mengikuti standar dan prosedur yang jelas

2.3. Sistem Pemrosesan Transaksi

Sistem pemrosesan transaksi atau biasa disebut *transaction processing system* (TPS) yang termasuk sistem informasi operasional merupakan jenis sistem informasi yang memiliki fokus pada data transaksi. Sistem informasi ini digunakan untuk menghimpun, menyimpan, dan memproses data transaksi serta kadangkala mengendalikan keputusan yang merupakan bagian dari transaksi. Contoh yang mengendalikan keputusan adalah sistem pemrosesan transaksi yang dapat memvalidasi keabsahan kartu kredit.

Karakteristik sistem pemrosesan transaksi menurut O'Brien yang dijelaskan dalam buku pengenalan sistem informasi oleh Kadir (2014) terdiri atas:

1. Sistem pemrosesan transaksi berfungsi mencatat data ke dalam basis data. Data yang dicatat meliputi data induk maupun data transaksi. Data Indk adalahan data yang lengkap dan dapat berdiri sendiri, misalnya data pegawai, data barang dagangan, data pelanggan. Data transaksi adalah data yang digunakan untuk mencatat transaksi. Transaksi adalah berbagai perubahan peristiwa yang terjadi dalam perusahaan.
2. Sistem pemrosesan transaksi digunakan oleh para pemakai akhir (end-user), yang terdiri atas operator(misalnya kasir di supermarket, teller di bank, resepsionis di hotel) atau para manajer pelaksanan.
3. Sistem pemrosesan transaksi menyajikan informasi atau laporan yang bersifat baku atau standar, tidak mengandung banyak variasi. Sebagai contoh, kasir di supermarket hanya akan menyediakan nota penjualan yang terdiri atas secarik kertas, demikian juga dengan informasi yang dihasilkan oleh mesin ATM.
4. Sistem pemrosesan transaksi diperlukan hampir setiap hari, karena di dalam suatu perusahaan, transaksi selalu terjadi. Setiap transaksi yang terjadi harus dicatat.

5. Sistem pemrosesan transaksi berguna untuk pembuatan keputusan terstruktur. Keputusan terstruktur adalah keputusan yang timbul karena masalah yang sudah jelas dan jalan keluarnya juga jelas, serta frekuensi kejadiannya sangat sering. Contoh keputusan terstruktur adalah penjualan tiket pesawat, pelayanan bank melalui ATM, dan pencatatan tagihan telepon.
6. Sistem pemrosesan transaksi memerlukan perangkat input dan output yang sangat bervariasi, mulai dari komputer, mesin ATM, telpon(baik telpon tetap maupun telpon seluler), dan perangkat lain, yang dalam masa depan akan semakin bervariasi dan semakin mudah digunakan.

Sedangkan menurut Turban, McLean, dan Wetherbe (1999) sistem pemrosesan transaksi mempunyai sejumlah karakteristik sebagai berikut:

1. Jumlah data yang diproses sangat besar
2. Sumber data umumnya internal dan keluaran terutama dimaksudkan untuk pihak internal (meskipun bisa juga diperuntukkan bagi mitra kerja)
3. Pemrosesan informasi dilakukan secara teratur: harian, mingguan, dan sebagainya
4. Kapasitas penyimpanan (basis data) besar
5. Kecepatan pemrosesan yang diperlukan tinggi karena volume yang besar
6. Umumnya memantau dan mengumpulkan data masa lalu
7. Masukan dan keluaran terstruktur. Mengingat data yang diproses cukup stabil, data diformat dalam suatu standar
8. Level kerincian yang tinggi mudah terlihat terutama pada masukan tetapi seringkali juga pada keluaran
9. Komputasi tidak rumit (menggunakan matematika sederhana atau operasi statistic)
10. Memerlukan keandalan yang tinggi
11. Pemrosesan terhadap permintaan merupakan suatu keharusan. Pemakai dapat melakukan permintaan terhadap basis data

Model sistem informasi ini dimulai dari data transaksi yang dimasukan kedalam sistem dan kemudian disimpan dalam basis data. Selanjutnya, sistem dapat memberikan laporan ataupun fokumen tentang transaksi. Pengguna juga dapat meminta suatu permintaan terhadap data dan sistem akan memberikannya. Pengguna juga dapat mengambil data (*download*) ataupun meletakkan data (*upload*) dalam basis data.

Kebijakan menggunakan sistem penjualan Alphapos dimulai sejak tahun 2000, dan diberlakukan di seluruh gerai PT Matahari Department Store. Sejak

diimplementasikan sistem informasi ini dapat lebih mudah untuk memberikan laporan penjualan mengenai kinerja setiap gerai kepada manajemen.

2.4. Risiko Teknologi Informasi

Risiko menurut Lientz & Larssen (2006) dapat didefinisikan sebagai kemungkinan bahaya, kerugian, atau kejahatan. Secara sistematis, risiko dapat melihat kemungkinan kerugian produk jika sebuah kejadian terjadi. Risiko terjadi karena dua komponen, yaitu celah dan ancaman.

Menurut Andrianto Moeljono (2016) Risiko Teknologi Informasi tidak hanya sebatas pada aset TI saja, dengan berkembangnya TI sebagai bagian dalam pengelolaan bisnis, maka risiko TI juga termasuk dengan kehilangan bisnis akibat kehilangan data, pelanggaran hukum dalam transaksi elektronik, bencana yang mengakibatkan terhentinya proses bisnis.

Dalam Stonebumer, Goguen, & Feringa (2002) dijelaskan bahwa penyebab risiko secara umum dibagi menjadi tiga bagian, yaitu:

a. Alam, seperti banjir, gempa bumi, tornado, longsor, longsor salju, badai petir, dan lain sebagainya
b. Manusia seperti kejadian yang disebabkan oleh aktivitas manusia seperti kelalaian dalam memasukan data, serangan pada jaringan, akses yang tidak sah untuk mengakses informasi penting
c. Lingkungan seperti gangguan listrik jangka panjang, polusi, bahan kimia, kebocoran zat cair

Lebih rinci dijelaskan oleh Andrianto Moeljono (2016) bahwa ancaman TI pada umumnya berkisar pada kondisi perangkat TI, seperti kegagalan perangkat lunak, virus, spam, phising, dan ancaman terbesar adalah kesalah manusia dalam pengelolaan sistem TI, pegelolaan data dan lain-lain. Ancaman TI yang mengarah pada tindakan pelanggaran hukum, misalnya serangan hacker, penipuan menggunakan sistem TI, pencurian kata kunci (*password*), serangan pada data, dan lain-lain. Sedangkan ancaman TI yang timbul akibat kejadian diluar normal, misalnya terjadinya bencana, baik bencana alam maupun bencana yang dibuat misalnya tindakan teroris.

2.5. Manajemen Risiko

Untuk meminimalisir risiko dibutuhkan manajemen risiko. Dimana manajemen risiko menurut ISO (2009) merupakan sekumpulan aktivitas untuk mengarahkan dan mengontrol sebuah organisasi dengan memperhatikan risiko. Manajemen risiko memberikan kontribusi kepada *good corporate governance* melalui pemberian jaminan yang wajar terhadap pencapaian sasaran organisasi melalui perlakuan risiko secara umum dan pengendalian risiko tersisa (*controlled residual risks*).

Manajemen risiko juga memberi perlindungan kepada pemangku jabatan terhadap akibat buruk yang mungkin terjadi karena adanya risiko. Hal ini dilakukan melalui perlakuan risiko sesuai prosedur manajemen risiko yang akan memberikan dua hal berikut: Pertama, dampak negatif yang terjadi tidak akan seburuk sebelumnya, karena telah dilakukan langkah-langkah antisipasi melalui proses perlakuan risiko. Kedua, dengan adanya manajemen risiko, para pemangku jabatan terkait dapat mengambil keputusan lebih baik (*informed decision*). Ini terjadi karena adanya informasi yang tersedia dalam proses manajemen risiko. Begitu juga bila risiko tesebut berdampak positif. Kesempatan untuk meraih peluang dapat diketahui lebih dulu dari pesaing sehingga dapat direbut.

PT Matahari Department Store berupaya memenuhi kode tata kelola perusahaan bedasarkan indikator-indikator yang diterapkan pada ASEAN *Corporate Governance Scorecard* (ACGS). Perusahaan menggunakan asesmen dari ACGS, selain juga proses pemantauan dan peninjauan internal yang dilakukan secara berkala, untuk mengidentifikasi hal-hal yang perlu diperbaiki sejalan dengan peraturan-peraturan dan GCG Roadmap yang diterbitkan oleh Otoritas Jasa Keuangan (OJK).

ASEAN *Corporate Governance Scorecard* (ACGS) memiliki lima area yang dikendalikan, yaitu hak pemegang saham, cara memperlakukan pemegang saham, peraturan untuk pemegang keputusan, transparansi dan pemberitahuan rahasia, serta tanggung jawab dewan. ACGS sendiri terdiri atas tiga tahap yaitu, tahap pengembangan awal, tahap penyempitan dan validasi, dan tahap pengembangan panduan secara rinci untuk penilai.

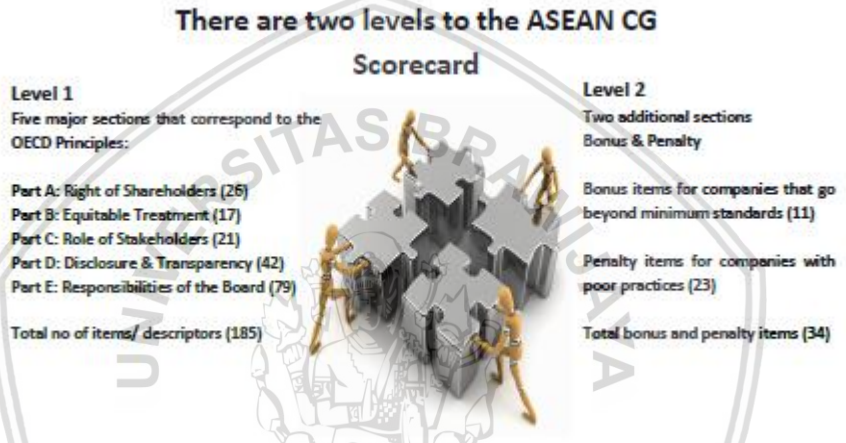
Tahap pengembangan awal akan digunakan sebagai patokan utama dalam mengembangkan *scorecard*, mengingat penerimaan globalnya oleh pembuat kebijakan, investor dan pemangku kepentingan lainnya. Akibatnya, banyak item dalam Scorecard mungkin praktik terbaik yang melampaui persyaratan perundang-undangan nasional. Para ahli juga menarik referensi dari badan kerja yang ada dan inisiatif peringkat di wilayah tersebut, termasuk yang oleh institut direksi, asosiasi pemegang saham dan universitas, untuk memandu pencantuman awal item dalam Scorecard.

Pada tahap penyempitan dan validasi, *scorecard* akan ditinjau bedasarkan setiap item dengan menggunakan prinsip OECD, prinsip dan praktik tata kelola perusahaan internasional lainnya yang direkomendasikan oleh badan seperti Bank Dunia, Jaringan Tata Kelola Korporat Internasional (ICGN), Asosiasi Tata Kelola Perusahaan Asia (ACGA) dan dipilih kode tata kelola perusahaan. *Scorecard* dimasukkan melalui proses validasi (disebut sebagai pengujian beta). Proses validasi juga berusaha mengidentifikasi sumber informasi untuk item Scorecard dan undang-undang, peraturan, dan aturan pencatatan yang berlaku

untuk setiap item untuk setiap negara. Scorecard juga dimasukkan melalui latihan peer-review untuk memastikan bahwa tidak akan ada perbedaan dalam standar penilaian yang diterapkan oleh masing-masing ahli.

Pada tahap akhir, tahap pengembangan panduan secara rinci, merupakan tahap untuk memastikan bahwa Scorecard diterapkan secara konsisten oleh semua penilai dan untuk memastikan konsistensi dalam penilaian di masa depan, catatan panduan rinci telah dikembangkan untuk masing-masing item, terutama jika item tersebut tidak jelas.

ACGS sendiri terdiri atas dua level yang memiliki fokus berbeda seperti pada gambar 2.3



Gambar 2. 3 Level pada ACG (Sumber : *ACMF, n.d.*)

Manajemen risiko dapat dikatakan telah terlaksana dengan baik bila proses manajemen risiko yang diuraikan dalam proses manajemen risiko telah terlaksanakan dengan baik di setiap tingkatan dan fungsi organisasi. Proses penerapan manajemen risiko ini merupakan bagian dari praktik-praktik terbaik organisasi dan proses bisnis organisasi.

2.6. Prinsip Manajemen Risiko

Menurut Susilo & Kaho (2017) Manajemen risiko suatu organisasi hanya dapat efektif bila mampu menganut prinsip-prinsip sebagai berikut:

1. Manajemen risiko melindungi dan menciptakan nilai tambah.
   Manajemen risiko memberikan kontribusi melalui peningkatan kemungkinan pencapaian sasaran perusahaan secara nyata. Selain itu, juga memberikan perbaikan dalam aspek keselamatan, kesehatan kerja, kepatuhan terhadap peraturan perundangan, perlindungan lingkungan hidup, persepsi public, kualitas produk, reputasi, *corporate governance*, efisiensi operasi, dan lain-lain
2. Manajemen risiko adalah bagian terpadu dari proses organisasi.

Manajemen risiko merupakan bagian dari tanggung jawab manajemen dan merupakan bagian tak terpisahkan dari proses organisasi, proyek, dan manajemen perubahan. Manajemen risiko bukanlah suatu aktivitas yang berdiri sendiri dan terpisah dari kegiatan serta proses organisasi dalam mencapai sasaran.

3. Manajemen risiko adalah bagian dari proses pengambilan keputusan.
   Manajemen risiko membantu para pengambil keputusan untuk mengambil keputusan atas dasar pilihan-pilihan yang tersedia dengan informasi yang selengkap mungkin. Manajemen risiko dapat membantu menentukan prioritas tindakan dan membedakan berbagai alternative tindakan. Manajemen risiko dapat membantu menunjukkan semua risiko yang ada, mana risiko yang dapat diterima dan mana risiko yang memerlukan perlakuan lebih lanjut. Manajemen risiko juga memantau apakah perlakuan risiko yang telah diambil memadai dan cukup efektif atau tidak. Informasi ini merupakan bagian dari proses pengambilan keputusan
4. Manajemen risiko secara khusus menangani aspek ketidakpastian.
   Manajemen risiko secara khusus menangani aspek ketidakpastian dalam proses pengambilan keputusan. Ia memperkirakan bagaimana sifat ketidakpastian dan bagaimanakah hal tersebut harus ditangani
5. Manajemen risiko bersifat sistematik, terstruktur, dan tepat waktu.
   Sifat sistematik, terstruktur, dan tepat waktu yang digunakan dalam pendekatan manajemen risiko inilah yang memberikan kontribusi terhadap efisiensi dan konsistensi manajemen risiko. Dengan demikian, hasilnya dapat dibandingkan dan memberikan hasil serta perbaikan
6. Manajemen risiko berdasarkan pada informasi terbaik yang tersedia.
   Masukan dan informasi yang digunakan dalam proses manajemen risiko didasarkan pada sumber informasi yang tersedia, seperti pengalaman, observasi, perkiraan, penilaian para ahli, dan data lain yang tersedia. Akan tetapi tetap harus disadari bahwa semua informasi ini mempunyai keterbatasan yang harus dipertimbangkan dalam proses pengambilan keputusan, baik dalam membuat model risiko maupun perbedaan pendapat yang mungkin terjadi di antara para ahli
7. Manajemen risiko adalah khas untuk penggunanya (*tailored*).
   Manajemen risiko harus diselaraskan dengan konteks internal dan ekternal organisasi, serta sasaran organisasi dan profil risiko yang dihadapi oleh organisasi tersebut
8. Manajemen risiko mempertimbangkan faktor manusia dan budaya.
   Penerapan manajemen risiko haruslah mengenali kapabilitas organisasi, persepsi dan tujuan masing-masing individu didalam serta diluar organisasi, khususnya yang menunjang atau menghambat pencapaian sasaran organisasi
9. Manajemen risiko harus transparan dan inklusif.

Untuk memastikan bahwa manajemen risiko tetap relevan dan terkini, para pemangku kepentingan dan pengambil keputusan di setiap tingkatan organisasi harus dilibatkan secara efektif. Keterlibatan ini juga harus memungkinkan para pemangku kepentingan terwakili dengan baik dan mendapatkan kesempatan untuk menyampaikan pendapat serta kepentingannya, terutama dalam merumuskan kriteria risiko

10. Manajemen risiko bersifat dinamis, berulang, dan tanggap terhadap perubahan.
    Ketika terjadi peristiwa baru, baik di dalam maupun di luar organisasi, konteks manajemen risiko dan pemahaman yang ada juga mengalami perubahan. Dalam situasi semacam inilah tahapan *monitoring* dan *review* berperan memberikan kontribusi. Risiko baru pun muncul, ada yang berubah, ada juga yang menghilang. Oleh karena itu, menjadi tugas manajemen untuk memastikan bahwa manajemen risiko senantiasa memerhatikan, merasakan, dan tanggap terhadap perubahan
11. Manajemen risiko harus memfasilitasi terjadinya perbaikan dan peningkatan organisasi secara berlanjut.
    Manajemen organisasi harus senantiasa mengembangkan dan menerapkan perbaikan strategi manajemen risiko serta meningkatkan kematangan pelaksanaan manajemen risiko sejalan dengan aspek lain dari organisasi

2.7. NIST SP 800-30

NIST 800-30 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko.

Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu (Syalim, Hori, dan Sakurai, 2009):

1. *System Characterization*
   Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.
2. *Threat Identification*
   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.
3. *Vulnerability Identification*
   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.

4. *Control Analysis*
   Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinankemungkinan pengembangan dari ancaman.
5. *Likelihood Determination*
   Proses rangking terhadap potensi dari kerawanandapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.
6. *Impact Analysis*
   Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.
7. *Risk Determination*
   Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini.
8. *Control Recommendations*
   Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem IT dan data, kepada tingkat risiko yang dapat diterima.
9. *Results Documentation*
   Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko yang dinilai dan kontrol yang direkomendasikan).

2.8. ISO 31000

Menurut Susilo & Kaho (2017), kesadaran mengenai pentingnya manajemen risiko telah menghasilkan berbagai macam standar mengenai manajemen risiko di berbagai Negara. Dengan adanya berbagai standar manajemen risiko dan consensus global tentang manajemen risiko, maka International Standard Organization mulai menyusun sebuah standar manajemen risiko, yaitu ISO 31000 *Risk Management – Guideline on principle implementation of risk management*. Setelah melalui proses *voting* dan revisi dari semua anggota ISO, standar ini akan diluncurkan menjadi standar internasional.

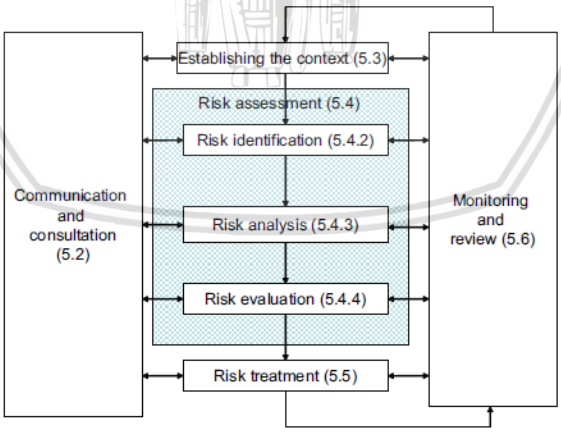
The International Organization for Standardization (ISO) 31000 Risk Management – Principles and Guidelines merupakan sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. Standar internasional yang diterbitkan pada 13 November 2009 ini dapat digunakan oleh segala jenis organisasi dalam menghadapi berbagai risiko yang melekat pada aktivitas mereka. Walau ISO 31000 menyediakan panduan generik, standar ini tidak ditujukan untuk menyeragamkan manajemen risiko lintas organisasi, tetapi

ditujukan untuk memberikan standar pendukung penerapan manajemen risiko dalam usaha memberikan jaminan terhadap pencapaian sasaran organisasi. ISO 31000 menyediakan prinsip, kerangka kerja, dan proses manajemen risiko yang dapat digunakan sebagai arsitektur manajemen risiko dalam usaha menjamin penerapan manajemen risiko yang efektif.

Satu hal yang membedakan ISO 31000 dengan standar manajemen risiko yang lain adalah perspektif ISO 31000 yang lebih luas dan lebih konseptual dibandingkan dengan yang lainnya. Hal ini ditandai dengan adanya prinsip-prinsip yang secara eksplisit dinyatakan. Juga adanya kerangka kerja manajemen risiko yang merupakan implementasi prinsip manajemen mutu dan dikenal dengan "*Plan-Do-Check-Action*". Dalam kerangka kerja manajemen risiko, hal ini dinyatakan dengan perencanaan kerangka kerja manajemen risiko, penerapan manajemen risiko, monitoring dan review, serta perbaikan berkelanjutan. Sedangkan proses manajemen risiko merupakan tahapan yang generic dan terdapat dalam berbagai standar maajemen risiko yang lainnya, yaitu identifikasi risiko, asesmen risiko, perlakuan terhadap risiko, serta implementasinya.

Standar ISO 31000 ini tidak dimaksudkan untuk proses sertifikasi. Sasaran penerapan manajemen risiko adalah untuk memastikan pencapaian sasaran organisasi melalui identifikasi hal-hal yang mengjambat atau peluang untuk meningkatkan pencapaian sasaran. Terhadap hambatan yang ada akan dilakukan asesmen, kemudian ditangani sehingga minimal. Terhadap peluang yang ada perlu juga dilakukan asesmen, kemudian dieksplorasi lebih lanjut untuk dimanfaatkan seoptimal mungkin.

2.7.1 Proses Manajemen Risiko



Gambar 2. 4 Proses manajemen risiko (Sumber : *ISO, 2009*)

Pada gambar 2.4 terlihat bahwa penentuan konteks berfungsi sebagai "filter" untuk menyaring berbagai macam risiko yang ada dan memisahkannya menjadi risiko yang relevan bagi organisasi. Sedangkan proses asesmen risiko akan menghasilkan profil risiko organisasi serta urutan prioritas kegawatan risiko.

Perlakuan risiko dengan empat pilihannya yaitu diterima, ditolak, berbagi dengan pihak lain, dan mitigasi akan menghasilkan risiko tersisa yang terkendali. Risiko-risiko ini harus selalu di-*monitor* dan di-*review*. Hasilnya akan menjadi masukan untuk perbaikan dan peningkatan efektifitas penerapan manajemen risiko.

Dalam menerapkan kerangka kerja manajemen risiko, organisasi hendaknya:

1. Menetapkan strategi dan waktu yang tepat untuk menerapkan kerangka kerja ini
2. Menerapkan kebijakan manajemen risiko dan proses manajemen risiko pada proses-proses organisasi
3. Mematuhi semua ketetapan peraturan perundangan yang berlaku
4. Mendokumentasikan proses pengambilan keputusan, termasuk proses penentuan sasaran yang sesuai dengan hasil dari proses manajemen risiko
5. Menyelenggarakan sosialisasi dan pelatihan manajemen risiko
6. Melakukan komunikasi dan konsultasi dengan para pemangku kepentingan untuk memastikan bahwa kerangka kerja manajemen risiko memang sesuai kebutuhan dan efektif

2.7.1.1. Komunikasi dan Konsultasi

Menurut Susilo & Kaho (2017) Komunikasi dan konsultasi menjadi penting karena manajemen risiko seharusnya dikembangkan oleh pihak-pihak yang telah sepaham mengenai hal ini. Selain itu, dimana diperlukan, mereka harus secara aktif terlibat dalam pengambilan keputusan mengenai penerapan kerangka kerja maupun proses manajemen risiko. Membangun kesepahaman, menyatukan visi ke depan, menginformasikan segala sesuatu mengenai teknik manajemen risiko, dan memfasilitasi penerapannya hanya dapat dilaksanakan dan memperoleh hasil yang optimal melalui perencanaan serta pelaksanaan komunikasi dan konsultasi yang efektif.

Komunikasi risiko tidak untuk menyelesaikan semua masalah atau konflik. Akan tetapi, yang perlu digarisbawahi adalah kekeliruan atau mengabaikan komunikasi risiko dapat berakibat hilangnya kepercayaan atau lemahnya pengelolaan risiko.

Konsultasi dapat dijelaskan sebagai suatu proses komunikasi antara perusahaan dengan para pemangku kepentingan, mengenai isu tertentu, terkait dengan pengambilan keputusan atau penentuan langkah tertentu dalam menangani suatu masalah. Konsultasi memiliki ciri-ciri sebagai berikut:

1. Merupakan proses, bukan hasil akhir
2. Berdampak terhadap suatu kepitisan melalui pengaruh ketimbang kekuasaan
3. Berhubungan dengan *input* terhadap pengambilan keputusan

Keseluruhan proses komunikasi dan konsultasi terdiri dari empat proses besar, yaitu persiapan, komunikasi eksternal, komunikasi internal, dan komunikasi berlanjut sepanjang pelaksanaan proses manajemen risiko.

2.7.1.2. Menentukan Konteks

Dengan ditetapkannya konteks berarti manajemen organisasi menentukan batasan atau parameter internal dan eksternal yang akan dijadikan pertimbangan dalam pengelolaan risiko, menentukan lingkup kerja, dan kriteria risiko untuk proses-proses selanjutnya. Konteks yang ditetapkan haruslah meliputi semua parameter internal dan eksternal yang relevan dan penting bagi organisasi. Dalam menetapkan konteks akan banyak ditemui kesamaan parameter dengan proses sebelumnya, yaitu ketika merencanakan kerangka kerja manajemen risiko. Akan tetapi, dalam proses manajemen risiko, parameter ini akan ditelaah jauh lebih rinci, khususnya yang terkait dengan lingkup suatu proses manajemen risiko tertentu.

A. Konteks Eksternal

Konteks eksternal adalah lingkungan ekternal dimana organisasi tersebut mengupayakan pencapaian sasaran yang ditetapkannya (Susilo & Kaho, 2017). Konteks eksternal dapat meliputi, tetapi tidak terbatas pada hal-hal berikut:

1. Lingkungan politik, sosial, ekonomi, budaya, keuangan, hukum, teknologi, dan keadaan alam, baik nasional, regional maupun internasional yang berpengaruh terhadap pencapaian sasaran organisasi
2. Faktor-faktor pendorong dan kecenderungan yang mempunyai dampak terhadap pencapaian sasaran organisasi
3. Persepsi dan nilai-nilai para pemangku kepentingan eksternal

B. Konteks Internal

Konteks internal menurut Susilo & Kaho (2017) adalah lingkungan internal dimana organisasi tersebut mengupayakan pencapaian sasaran yang ditetapkannya. Proses manajemen risiko haruslah diselaraskan dengan budaya, proses, dan struktur organisasi. Konteks internal adalah segala sesuatu didalam organisasi yang dapat mempengaruhi cara organisasi dalam mengelola risiko. Penting untuk memahami konteks internal ini dalam pengertian misalnya sebagai berikut:

1. Kapabilitas organisasi dalam pengertian sumber daya dan sumber pengetahuan yang dimiliki (misalnya modal, waktu, orang, sistem, proses, dan teknologi)
2. Sistem informasi, alur komunikasi, dan proses pengambilan keputusan, baik yang formal maupun informal
3. Para pemangku kepentingan internal
4. Kebijakan, sasaran, dan strategi untuk mencapainya
5. Persepsi, nilai-nilai, dan budaya organisasi
6. Standar dan model acuan yang diadopsi organisasi

7. Struktur (*governance*, peran, dan akuntabilitas)

C. Konteks Proses Manajemen Risiko

Konteks proses manajemen risiko menurut Susilo & Kaho (2017) adalah konteks dimana proses manajemen risiko diterapkan. Konteks proses manajemen risiko akan berubah sesuai dengan kebutuhan organisasi. Hal ini dapat meliputi, tetapi tidak terbatas pada hal-hal sebagai berikut:

1. Penetapan tanggung jawab untuk proses manajemen risiko
2. Penetapan lingkup kegiatan manajemen risiko, baik dari luas maupun kedalamannya, termasuk bila ada hal-hal khusus yang harus diperhatikan atau tidak dicakup
3. Penentuan tujuan, sasaran, lokasi, maupun tempat dari kegiatan, proses, fungsi, proyek, produk jasa dan harta yang terkena kegiatan manajemen risiko
4. Penentuan hubungan dari proyek atau kegiatan khusus organisasi dengan proyek dan kegiatan lain organisasi
5. Penentuan metode untuk melakukan asesmen risiko
6. Penentuan kriteria penilaian kinerja manajemen risiko
7. Melakukan identifikasi dan spesifikasi keputusan-keputusan yang harus diambil
8. Melakukan identisikasi, lingkup, ataupun kerangka kajian studi yang diperlukan, termasuk luas dan sasarannya serta sumber daya yang diperlukan untuk melakukan kajian tersebut

2.7.1.3. Asesmen Risiko

A. Identifikasi Risiko

Tahapan ini bertujuan untuk mengidentifikasi risiko yang harus dikelola organisasi melalui proses yang sistematis dan terstruktur. Proses ini sangat penting karena risiko yang tiak teridentifikasi pada proses ini tidak akan ditangani pada proses-proses selanjutnya. Proses ini juga harus mengupayakan untuk mengidentifikasikan risiko-risiko, baik yang dalam kendali organisasi maupun diluar kendali organisasi (eksternal).

Proses tersebut dimulai dengan mengidentifikasikan secara komprehensif, ekstensif, dan intensif mengenai risiko apa saja yang dapat terjadi, dimana, dan bilamana. Setelah diperoleh daftar risiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana terjadinya.

Sasaran identifikasi risiko adalah mengembangkan daftar sumber risiko dan kejadian yang komprehensif serta memiliki dampak terhadap pencapaian sasaran dan target (atau elemen kunci) yang teridentifikasi dari konteks (Susilo & Kaho, 2017). Dokumen utama yang dihasilkan dalam proses ini adalah daftar risiko (*risk register*).

Dalam proses identifikasi risiko, informasi yang dikumpulkan antara lain mencakup:

1. Sumber risiko meliputi *stakeholder*, benda, atau kondisi lingkungan yang dapat memicu timbulnya risiko
2. Kejadian meliputi peristiwa yang dapat terjadi dan berdampak terhadap pencapaian sasaran dan target
3. Konsekuensi meliputi dampak terhadap aset organisasi atau *stakeholder*
4. Pemicu (apa dan mengapa) meliputi faktor-faktor yang menjadi pemicu timbulnya suatu peristiwa berisiko
5. Pengendalian meliputi langkah-langkah antisipasi dan pencegahan awal yang dapat dilaksanakan
6. Perkiraan kapan risiko terjadi dan dimana risiko itu dapat terjadi

B. Analisis Risiko

Analisis risiko menurut Susilo & Kaho (2017) adalah upaya untuk memahami risiko lebih dalam. Hasil analisis risiko ini akan menjadi masukan bagi evaluasi risiko dan proses pengambilan keputusan mengenai perlakuan terhadap tersebut. Analisis risiko meninjau dua aspek risiko, yaitu dampak dan kemungkinannya. Tingkat risiko akan ditentukan oleh kombinasi yang digunakan harus konsisten dengan kriteria risiko yang ditetapkan sebelumnya.

Tujuan dari analisis risiko adalah melakukan analisis dampak dan kemungkinan semua risiko yang dapat menghambat tercapainya sasaran organisasi, juga semua peluang yang mungkin dihadapi organisasi. Kondisi ini dicapai apabila beberapa hal berikut dapat dipenuhi:

1. Proses analisis risiko dilaksanakan secara komprehensif dan mencakup semua risiko serta peluang yang ditemui dalam proses identifikasi risiko sebelumnya dan telah masuk ke dalam daftar risiko
2. Semua yang terkait dengan risiko tersebut (para pemangku risiko) telah terlibat dalam proses analisis dan melakukan analisis berdasarkan informasi, data, serta pengetahuan yang mereka miliki dengan baik
3. Proses analisis ini didampingi atau ditunjang dengan pengetahuan mengenai manajemen risiko yang memadai
4. Waktu yang dialokasikan untuk proses ini cukup memadai
5. Ukuran kemungkinan dan dampak yang digunakan harus konsisten dan sesuai dengan organisasi tersebut. Apabila digunakan tabel kemungkinan dan dampak, besaran dan pengelompokan nilai yang digunakan hendaknya tidak terlalu lebar dan juga tidak terlalu sempit, tetapi sesuai dengan organisasi tersebut

C. Evaluasi Risiko

Tujuan dari evaluasi risiko menurut Susilo & Kaho (2017) adalah membantu proses pengambilan keputusan berdasarkan hasil analisis risiko. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaiman prioritas perlakuan atas risiko-risiko tersebut. Hasil evaluasi risiko akan menjadi masukan bagi proses perlakuan risiko.

2.7.1.4. Perlakuan Risiko

Menurut Stonebumer, Goguen, & Feringa (2002) perlakuan risiko merupakan proses manajemen risiko yang melibatkan prioritas, evaluasi, dan menerapkan pengendalian risiko yang sesuai dengan rekomendasi dari penilaian risiko. Karena penghapusan risiko tidak praktis atau mendekati tidak mungkin, maka hal tersebut merupakan tanggung jawab manajemen senior dan manajer fungsional serta bisnis untuk menggunakan biaya terendah dalam penerapan kontrol yang paling tepat untuk mengurangi risiko ke tingkat yang dapat diterima dengan meminimalisasi dampak yang diterima perusahaan.

Menurut Susilo & Kaho (2017) terdapat beberapa pilihan yang ada dalam perlakuan risiko diantaranya:

1. *Risk avoidance*, digunakan untuk menghindari risiko dengan menghilangkan penyebab dan atau konsekuensi risiko. Misalnya, mematikan beberapa fungsi sistem atau keseluruhan sistem saat risiko teridentifikasi.
2. *Risk reduction,* digunakan dengan mengurangi kemungkinan atau dampak. Misalnya, pendidikan dan pelatihan bagi tenaga kerja untuk menghadapi risiko yang terjadi, perlindungan terhadap personil serta properti yang ada.
3. *Risk acceptance*, dapat menerima risiko yang berarti sama dengan menanggung seluruh tanggung jawab atas risiko yang terjadi. Misalnya, tidak menggunakan mengasuransikan server terhadap risiko kerusakan dan akan bersedia menanggung kerugian jika risiko kerusakan terhadap servernya.
4. *Risk sharing*, digunakan untuk mentransfer risiko dengan menggunakan opsi lain untuk mengurangi dampak, seperti membeli asuransi.

Maka dalam menentukan pilihan perlakuan risiko, perlu diperhatikan beberapa hal, yaitu:

1. Bagaimana pengaruh perlakuan risiko yang dipilih terhadap kemungkinan terjadinya risiko atau dampak yang ditimbulkan oleh risiko tersebut. Pengaruh dari perlakuan ini juga harus dipertimbangkan dengan toleransi atau selera risiko organisasi
2. Pertimbangan biaya dengan manfaat dari perlakuan risiko yang dipilih
3. Bagaimanakah kemungkinan pencapaian sasaran organisasi dengan adanya perlakuan risiko tersebut

2.7.1.5. Monitoring dan Review

Monitoring adalah pemantauan rutin terhadap kinerja actual proses manajemen risiko dibandingkan dengan rencana atau harapan yang akan dihasilkan. Sedangkan *review* adalah peninjauan atau pengkajian berskala atas kondisi saat ini dengan fokus tertentu, misalnya efektivitas pengendalian

terhadap risiko keuangan atau risiko pasar, atau bagimana mempertajam analisis risiko saat ini.

Proses *monitoring* dan *review* harus mencakup semua aspek dari proses manajemen risiko dengan tujuan agar:

1. Terdapat proses pembelajaran dan analisis dari setiap peristiwa, perubahan, dan kecenderungan (*trends*) yang terjadi
2. Terdeteksi perubahan dalam lingkup internal maupun eksternal, termasuk perubahan risiko itu sendiri yang memerlukan perubahan atau revisi perlakuan risiko, atau bahkan perubahan prioritas risiko
3. Memastikan bahwa pengendalian risiko dan perlakuan risiko masih tetap efektif, baik secara desain maupun pelaksanaannya
4. Mengidentifikasikan terjadinya risiko-risiko yang baru

2.8. Aset Pendukung Sistem Informasi

Menurut Stonebumer, Goguen, & Feringa (2002) aset yang terdapat di dalam semua jenis sistem informasi mencakup empat poin. Berikut keempat aset tersebut beserta dengan penjelasannya masing-masing:

1. *Software* (perangkat lunak)
   Komponen *software* mencakup semua perangkat lunak yang digunakan didalam sistem informasi. Adanya komponen perangkat lunak ini akan membantu sistem informasi di dalam menjalankan tugasnya dan untuk dapat dijalankan sebagaimana mestinya. Komponen perangkat lunak ini melakukan proses pengolahan data, penyajian informasi, perhitungan data, dan lain-lain. Komponen perangkat lunak mencakup sistem operasi, aplikasi, dan driver.
2. *Hardware* (perangkat keras)
   Komponen *hardware* mencakup semua perangkat keras computer yang digunakan secara fisik di dalam sistem informasi, baik computer server maupun computer klien. Komponen perangkat keras ini meliputi computer server beserta komponen di dalamnya, komputer desktop beserta komponen didalamnya, computer jinjing beserta komponen di dalamnya, mobile device (tablet, smartphone) dan lain-lain. Termasuk juga didalamnya hub, switch, router, yang berperan di dalam jaringan computer.
3. Personil
4. Informasi

Sedangkan menurut Stergiopoulos, Gritzalis, & Kouktzoglou (2018) aset pendukung memiliki kerentanan yang dapat dieksploitasi dengan ancaman yang bertujuan untuk mengganggu aset utama dari ruang lingkup (proses dan informasi). Jenis aset pendukung ditunjukkan di bawah ini.

1. *Hardware*
   Jenis perangkat keras terdiri dari semua elemen fisik mendukung proses
2. *Software*
   Software terdiri dari semua program yang berkontribusi pada pengoperasian perangkat pengolahan data.
3. Jaringan
   Jenis jaringan terdiri dari semua telekomunikasi Perangkat yang digunakan untuk menghubungkan beberapa *remote* fisik komputer atau elemen sistem informasi.
4. Personil
   Tipe personel terdiri dari semua kelompok orang terlibat dalam sistem informasi.
5. Situs
   Jenis situs terdiri dari semua tempat yang berisi ruang lingkup atau bagian dari ruang lingkup, dan sarana fisik yang diperlukan untuk itu beroperasi.
6. Organisasi
   Tipe organisasi menggambarkan kerangka kerja organisasi, terdiri dari semua struktur personalia yang ditugaskan untuk tugas dan prosedur yang mengendalikan struktur ini.

2.9 *Likelihood*

Menurut Susilo & Kaho (2017) kemungkinan sering dinyatakan dengan probabilitas, yaitu suatu angka antara 0 dan 1. Angka 0 menyatakan bahwa kejadian yang dimaksud tidak mungkin terjadi, sebaliknya angka 1 menyatakan bahwa hal tersebut pasti terjadi. Akan tetapi, tidak ada yang absolut sehingga ketidakpastian tersebut dinyatakan dalam angka diantara 0 dan 1.

Sedangkan menurut Stonebumer, Goguen, & Feringa (2002) *likelihood* merupakan potensi kerentanan yang dapat dilakukan oleh sumber ancaman tertentu. Tingkat kemungkinan digambarkan sebagai tiga tingkatan sebagai berikut:

Tabel 2. 1 Tingkatan *likelihood*

Rating likelihood	Kriteria *likelihood*	Definisi *likelihood*
A	Tinggi	Sumber ancaman memiliki motivasi dan kemampuan namun kontrol yang ada tidak efektif untuk mencegah ancaman
B	Sedang	Sumber ancaman memiliki motivasi dan kemampuan namun kontrol yang ada mampu untuk menghambat ancaman
C	Rendah	Sumber ancaman tidak memiliki motivasi atau kemampuan atau kontrol yang ada mampu untuk menghalangi ancaman

(Sumber : Stonebumer, et al., 2002)

2.11 Dampak Risiko

Beberapa dampak nyata dapat diukur secara kuantitatif dalam pendapatan yang hilang, biaya untuk memperbaiki sistem, atau tingkat upaya yang diperlukan untuk memperbaiki masalah yang disebabkan oleh tindakan ancaman yang sukses. Dampak lain (misalnya, hilangnya kepercayaan publik, hilangnya kredibilitas, kerusakan pada organisasi bunga) tidak dapat diukur dalam satuan tertentu tetapi dapat dikualifikasi atau dijelaskan dalam hal tinggi, sedang, dan berdampak rendah. Karena sifat umum dari diskusi ini, panduan ini menunjukkan dan hanya menggambarkan kategori kualitatif — dampak tinggi, sedang, dan rendah.

Tabel 2. 2 Tingkat dampak risiko

Kriteria *magnitude of impact*	Definisi *magnitude of impact*
Tinggi	Sumber ancaman menyebabkan nilai kehilangan yang tinggi pada aset ataupun sumber daya, secara signifikan melanggar misi ataupun reputasi organisasi, menyebabkan korban jiwa
Sedang	Sumber ancaman menyebabkan nilai kehilangan pada aset ataupun sumber daya, secara signifikan melanggar misi ataupun reputasi organisasi, menyebabkan korban jiwa
Rendah	Sumber ancaman menyebabkan nilai kehilangan yang tinggi pada aset ataupun sumber daya, secara signifikan melanggar misi ataupun reputasi organisasi

(Sumber : Stonebumer, et al., 2002)

2.12 Matriks Level Risiko

Menurut Stonebumer, Goguen, & Feringa (2002) matriks level risiko merupakan penentuan akhir nilai risiko yang diturunkan dengan mengalikan nilai *likehood* dengan nilai dampak dari setiap ancaman. Matriks yang digunakan berikut merupakan matriks 3x3 dengan rincian *likelihood* (tinggi, sedang, dan rendah) serta dampak ancaman (tinggi, sedang, dan rendah). Pada penentuan level risiko ini mungkin subjektif. Sehingga diperlukan alasan pembenaran yang dapat dijelaskan dalam setiap nilai *likelihood* dan *magnitude of impact.*

Tabel 2. 3 Matrik Level Risiko

Likelihood	*Impact*		
	Rendah (10)	Sedang (50)	Tinggi (100)
Tinggi (1,0)	Rendah 10 x 0,1 = 10	Sedang 50 x 1,0 = 50	Tinggi 100 x 1,0 = 100
Sedang (0,5)	Rendah 10 x 0,5 = 5	Sedang 50 x 0,5 = 25	Sedang 100 x 0,5 =50
Rendah (0,1)	Rendah 10 x 0,1 = 1	Rendah 50 x 0,1 = 5	Rendah 100 x 0,1 = 10

(Sumber : *Stonebumer, et al., 2002*)

Setelah perhitungan matriks level risiko, maka setiap risiko akan diperingkatkan dengan nilai tinggi, sedang, dan rendah. Pada hasil ini akan menampilkan derajat level risiko sistem, fasilitas, atau prosedur yang dilaksanakan.

Tabel 2. 4 Skala risiko dan tindakan yang diperlukan

Risk Level	*Risk Description and Necessary Actions*
High	*If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.*
Medium	*If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.*
Low	*If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.*

(Sumber : *Stonebumer, et al., 2002*)

2.13 Identifikasi Kelemahan Sistem

Pada tahap ini, menentukan apakah persyaratan keamanan yang ditetapkan untuk sistem TI dan dikumpulkan selama karakterisasi sistem telah terpenuhi oleh kontrol keamanan yang ada atau yang direncanakan. Biasanya, persyaratan keamanan sistem bisa jadi disajikan dalam bentuk tabel. Daftar periksa persyaratan keamanan berisi standar keamanan dasar yang dapat digunakan secara sistematis mengevaluasi dan mengidentifikasi kerentanan aset, prosedur, proses, dan transfer informasi yang tidak terarah. Bidang keamanan pada sistem TI sebagai berikut:

1. Manajemen
2. Operasional

3. Teknis

2.14 Rekomendasi Pengendalian

Menurut Moningka (2016) *human error* (kesalahan dalam mengoperasikan sistem) merupakan *error* atau kesalahan yang dilakukan oleh manusia yang merupakan perilaku kurang sesuai yang pada akhirnya menghambat tercapainya suatu tujuan. Yang mana juga mengemukakan diperlukan hal-hal sebagai berikut untuk meminimalisir kesalahan yang terjadi, diantaranya mendesain atau menyusun Prosedur operasi (SOP), analisa kebutuhan training, dibentuk team atau kelompok kerja, diatur alokasi penggunaan manusia dan mesin, mendesain panel kontrol untuk kerja, melakukan analisa beban kerja, serta analisa terhadap human error yang terjadi untuk dijadikan umpan balik. Dan didukung dengan kutipan mengenai penangan risiko dari Redaksi (2015) terdapat 4 cara untuk memperbaiki kesalahan yang diakibatkan oleh *human error* yang dijabarkan oleh Antonio Ferraro, praktisi Lean. 4 cara tersebut yaitu menangkap kesalahan lebih awal, memberikan pelatihan yang tepat, menemukan akar penyebab masalah, dan bekerja sama.

Risiko tidak dijalankannya tata kelola disebabkan oleh tidak dijalankannya kode etik dan tanggung jawab profesional. Menurut PT Link Net Tbk (2014) penanganan terhadap penyimpangan atas peraturan perusahaan dan kode etik dan tanggung jawab profesional dilakukan melalui penyelidikan yang mendalam dan didasari dengan fakta-fakta, sedangkan keputusannya dibuat dan diberikan berdasarkan pertimbangan akibat tindakan. Sehingga dalam pengendaliannya menggunakan sanksi kepada karyawan. Sanksi yang diberikan berupa teguran lisan, surat peringatan, tidak diberikan kenaikan gaji, pangkat, atau bonus, hingga pemutusan hubungan kerja.

Lalu dalam penelitian Sari, Papilaya, & Manuputty (2017) yang berjudul Evaluasi Pengendalian Aplikasi pada Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA) menunjukan bahwa pengendalian untuk pencurian *password* yang disebabkan *password* yang mudah ditebak adalah diberlakukan format khusus dalam pembuatan *password*. Sedangkan pengendalian untuk pencurian *password* yang disebabkan oleh percobaan peretasan aplikasi dengan menebak *Username* dan *password User* dengan menggunakan peran *admin* dalam memonitor *log login* sistem aplikasi.

Menurut Mahersmi, Muqtadiroh, & Hidayanto (2016) dalam penelitian yang berjudul Analisis Risiko Keamanan Informasi dengan Menggunakan Metode Octave dan Kontrol ISO 27001 pada DISHUBKOMINFO Kabupaten Tulungagung menghasilkan bahwa risiko *network failure* yang berupa koneksi internet tidak stabil dapat menggunakan pengendalian berupa tindakan kontrol jaringan

dengan cara dimonitoring serta memelihara keamanan sistemnya yang ditinjau secara berkala.

2.15. Teknik Pengumpulan Data

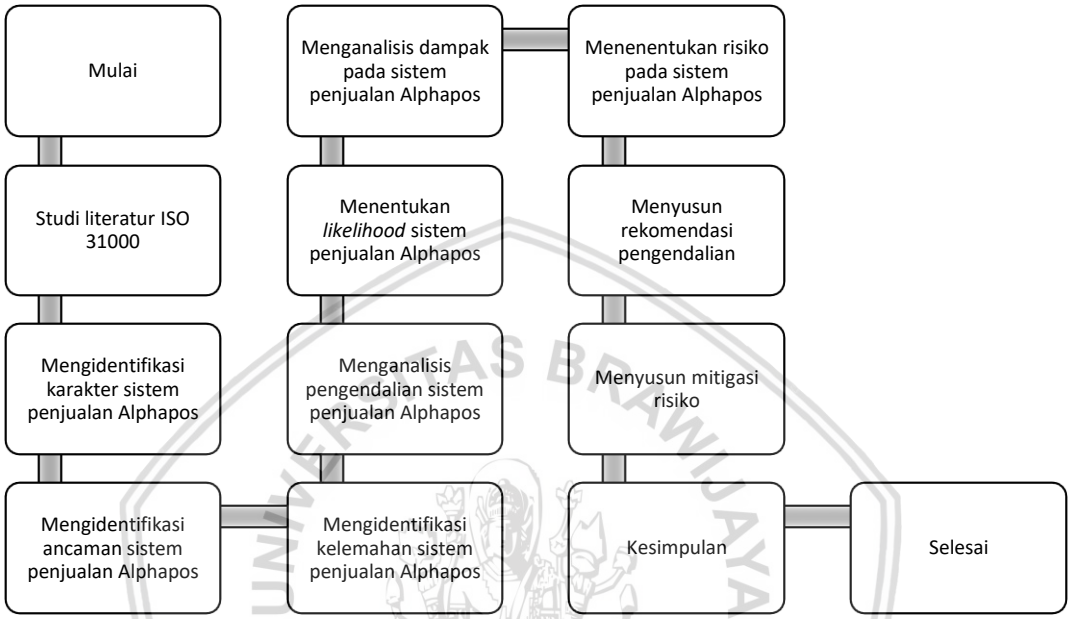
Beberapa teknik dapat digunakan untuk mengumpulan informasi yang berhubungan dengan sistem TI, seperti :

1. Kuisioner. Untuk mengumpulkan informasi yang relevan, personel penilaian risiko dapat membuat kuesioner atau daftar pertanyaan tentang manajemen dan pengendalian operasional yang direncanakan atau yang telah digunakan untuk sistem TI. Kuisioner ini harus didistribusikan ke yang berlaku tenaga manajemen teknis dan non-teknis yang merancang atau mendukung sistem TI. Kuesioner juga dapat digunakan selama kunjungan di lokasi dan wawancara.
2. Wawancara di tempat (*on site interviews*). Wawancara dengan dukungan sistem TI dan personel manajemen dapat memungkinkan personel penilaian risiko untuk mengumpulkan informasi yang berguna tentang TI sistem (misalnya, bagaimana sistem dioperasikan dan dikelola). *On site interviews* juga memungkinkan personel penilaian risiko untuk mengamati dan mengumpulkan informasi tentang fisik, keamanan lingkungan, dan operasional sistem TI.
3. Meninjau Dokumen. Dokumen kebijakan (misalnya, dokumentasi legislatif, arahan), dokumentasi sistem (misalnya, panduan pengguna sistem, panduan administratif sistem, desain sistem dan dokumen persyaratan, dokumen akuisisi), dan terkait keamanan dokumentasi (misalnya, laporan audit sebelumnya, laporan penilaian risiko, hasil pengujian sistem, rencana keamanan sistem, kebijakan keamanan) dapat memberikan informasi yang baik tentang kontrol keamanan yang digunakan oleh dan direncanakan untuk sistem TI. Misi organisasi analisis dampak atau penilaian kritikalitas aset menyediakan informasi mengenai sistem dan kekritisan data dan sensitivitas.
4. Menggunakan Alat Pemindaian Otomatis. Metode teknis proaktif dapat digunakan untuk mengumpulkan informasi sistem secara efisien. Sebagai contoh, alat pemetaan jaringan bisa mengidentifikasi layanan yang berjalan pada sekelompok besar host dan menyediakan cara cepat membangun profil individu dari sistem TI target.

BAB 3 METODOLOGI PENELITIAN

3.1 Metode Penelitian

Pada penelitian skripsi ini bersifat kualitatif dengan menggunakan metode penelitian sebagai berikut



Gambar 3. 1 Metodologi Penelitian

Dalam melakukan penelitian ini ada beberapa langkah yang harus dilakukan sesuai dengan mengikuti risk assessment dari literatur Stonebumer, Goguen, & Feringa (2002). Langkah-langkah penelitian ini adalah sebagai berikut:

1. Mulai
2. Studi literature ISO 31000
3. Mengidentifikasi karakter sistem penjualan Alphapos
4. Mengidentifikasi ancaman sistem penjualan Alphapos
5. Mengidentifikasi kelemahan sistem penjualan Alphapos
6. Menganalisis pengendalian sistem penjualan Alphapos
7. Menentukan *likelihood* sistem penjualan Alphapos
8. Menganalisis dampak pada sistem penjualan Alphapos
9. Menenentukan risiko pada sistem penjualan Alphapos
10. Menyusun rekomendasi pengendalian
11. Menyusun mitigasi risiko
12. Kesimpulan
13. Selesai

3.2. Studi Literatur ISO 31000

Untuk memulai penelitian ini maka dimulai dengan mempelajari literatur penunjang seperti manajemen risiko menurut ISO 31000 dengan ditunjang literatur mengenai NIST 800-30 yang lebih menspesifikasikan dalam memanajemen risiko pada teknologi informasi.

3.3. Mengidentifikasi karakter sistem penjualan Alphapos

Pada tahap ini mengumpulkan data yang berkaitan sistem penjualan Alphapos berupa perangkat keras, perangkat lunak, keamanan sistem, dan fungsi dari sistem tersebut. Hal ini dilakukan agar mengetahui batasan-batasan sistem penjualan Alphapos, seperti *hardware, software, system interfaces,* data dan informasi, personil yang *support* dan menggunakan sistem, fungsi sistem, serta kekritisan dan sensitivitas sistem dan data. Pada tahap ini menggunakan metode pengumpulan data *on site interviews* dengan personil manajemen serta personil yang menangani sistem tersebut (tim EDP).

3.4. Mengidentifikasi ancaman sistem penjualan Alphapos

Pada tahap ini dilaksanakan dengan *one site interviews.* Pada tahap ini berguna untuk mengetahui sumber risiko pada sistem penjualan perusahaan serta bentuk ancaman dari setiap sumber risiko tersebut. Yang mana data tersebut berfungsi untuk memperhitungkan *likelihood* serta dampak dari setiap risiko.

3.5. Mengidentifikasi kelemahan sistem penjualan Alphapos

Pada tahap ini juga dilaksanakan dengan *on site interviews*. Pada tahap ini berguna untuk menentukan daftar kelemahan sistem yang berpotensi untuk menjadi sumber dari risiko. Sehingga dapat menjadi bahan pertimbangan untuk menyusun rekomendasi pengendalian yang tepat untuk setiap risiko. Pada tahap ini juga mengumpulkan data mengenai kerentanan sistem.

Karena sistem penjualan sudah dan sedang beroperasi maka identifikasi kerentanan diperluas untuk memasukkan informasi yang lebih spesifik, seperti fitur keamanan yang direncanakan dan dijelaskan dalam dokumentasi desain keamanan, kontrol keamanan, teknis dan prosedural yang digunakan untuk melindungi sistem.

Sebagai penunjang sumber kerentanan yang harus dipertimbangkan dalam analisis kerentanan menyeluruh meliputi dokumentasi penilaian risiko sebelumnya, laporan audit sistem, laporan anomali sistem, laporan uji dan evaluasi sistem, daftar kerentanan.

Pada tahap ini, personil penilaian risiko akan menentukan apakah persyaratan keamanan ditetapkan untuk sistem TI dan dikumpulkan selama

karakterisasi sistem dipenuhi oleh kontrol keamanan yang ada atau direncanakan. Oleh karena itu pada hasil akhir tahap ini akan dihasilkan dalam bentuk table, dengan setiap persyaratan disertai penjelasan tentang bagaimana desain atau implementasi sistem.

3.6. Menganalisis pengendalian sistem penjualan Alphapos

Pada tahap ini dilakukan *checklist* untuk membuat daftar pengendalian yang telah dilaksanakan oleh perusahaan. Pada tahap ini bertujuan untuk menganalisis pengendalian yang telah ada atau yang telah direncanakan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan ancaman menggunakan kerentanan sistem. Pelaksanaan pengendalian saat ini atau yang direncanakan harus dipertimbangkan. Oleh karena itu, pembaharuan daftar periksa tersebut untuk mencerminkan perubahan dalam lingkungan kontrol organisasi untuk memastikan validitas daftar periksa.

3.7. Menentukan *likelihood* sistem penjualan Alphapos

Pada tahap ini dilaksanakan untuk mendapatkan peringkat *likelihood* yang mengindikasikan probabilitas bahwa sumber ancaman berpotensi dapat melakukan ancaman. Dalam tahap ini dikumpulkan data mengenai motivasi dan kemampuan sumber ancaman, sifat kerentanan, serta keberadaan dan efektivitas kontrol yang ada saat ini. Pada tahap ini dilaksanakan dengan metode *on site interviews* kepada personil manajemen dan personil IT yang ada di perusahaan. Lalu dari hasil *interview* akan dikonversikan kedalam nilai tinggi, sedang, atau rendah.

3.8. Menganalisis dampak pada sistem penjualan Alphapos

Langkah utama selanjutnya adalah menentukan dampak buruk yang diakibatkan sebuah ancaman yang berhasil dilakukan. Pada tahap ini dilaksanakan dengan metode *document review* dan wawancara. Sebelum memulai analisis dampaknya diperlukan informasi penting seperti misi sistem, kekritisan sistem dan data, serta sensitivitas sistem dan data.

Jika dokumentasi tesebut tidak ada maka dapat ditentukan bedasarkan tingkat perlindungan yang dibutuhkan untuk menjaga sistem dan ketersediaan data, integritas, dan kerahasiaan. Terlepas dari metode yang digunakan untuk mengetahui seberapa sensitive sistem dan data, pemilik sistem bertanggung jawab untuk menentukan tingkat dampaknya sendiri. Sehingga dalam menganalisa dampaknya, pendekatan yang tepat adalah mewawancarai pemilik sistem. Pada hasil akhir tahap ini akan disajikan dengan kategori kualitatif seperti tinggi, sedang, dan rendah.

3.9. Menenentukan risiko pada sistem penjualan Alphapos

Pada tahap ini digunakan untuk menilai tingkat risiko terhadap sistem penjualan Alphapos. Penentuan risiko dinilai dari pengumpulan data pada tahap sebelumnya seperti *likelihood* serta dampak yang dihasilkan dari setiap risiko. Sehingga pada tahap ini akan menghasilkan peringkat risiko yang terjadi pada sistem penjualan Alphapos.

Dalam menentukan risiko apa saja yang termasuk dalam penelitian ini dibantu dengan mengkategorikan dengan risiko setiap aset yang terdiri atas personil, perangkat keras, perangkat lunak, dan data. Lalu dibantu dengan hasil studi literatur mengenai risiko yang terdapat pada bidang teknologi informasi.

Hasil pada tahap ini akan disajikan dalam bentuk tabel dan akan diperingkatkan dengan nilai akhir yaitu hasil perkalian antara nilai *likelihood* dengan nilai dampak pada setiap risiko. Sehingga dari hasil tersebut dapat menyimpulkan top IT risk yang akan diberikan rekomendasi pengendalian dan menjadi risiko prioritas yang akan dibahas pada tahap selanjutnya.

3.10. Menyusun rekomendasi pengendalian

Tujuan dari merekomendasikan pengendalian terhadap sistem penjualan Alphapos adalah untuk mengurangi tingkat risiko terhadap sistem penjualan dan datanya ke tingkat yang dapat diterima. Rekomendasi pengendalian merupakan hasil dari proses penilaian risiko dan memberikan masukan kepada perusahaan untuk menentukan mana yang dibutuhkan oleh perusahaan. Pada tahap ini akan menghasilkan daftar rekomendasi pengendalian dengan bantuan dari penelitian sebelumnya serta literatur untuk menentukan opsi rekomendasi pengendalian apa saja yang patut untuk diangkat.

3.11. Menyusun mitigasi risiko

Pada tahap ini akan dilakukan perhitungan dengan *cost benefit analysis* dari setiap opsi rekomendasi pengendalian yang akan menghasilkan rekomendasi pengendalian prioritas yang memiliki *benefit* terbesar. Dari perhitungan *cost benefit analysis* akan diketahui *cost* ketika mengimplementasikan rekomendasi pengendalian serta *benefit* yang akan didapat ketika rekomendasi pengendalian tesebut di terapkan.

3.12. Kesimpulan

Kesimpulan berisi hasil penelitian yang telah dilakukan, mencakup identifikasi risiko, peringkat risiko, serta mitigasi risiko yang ada di Matahari Department Store yang mana diharapkan dapat digunakan sebagai acuan perbaikan di masa mendatang. Pada bagian ini juga akan dijelaskan mengenai saran-saran yang dapat diberikan untuk penelitian selanjutnya.

BAB 4 PENGUMPULAN DATA

4.1. Observasi

Observasi dilakukan untuk melengkapi kebutuhan informasi mengenai manajemen risiko pada PT Matahari Department Store. Observasi dilakukan dengan pengamatan terhadap proses bisnis yang ada dan apa saja masalah yang ada pada perusahaan.

Dari hasil observasi di PT Matahari Department Store didapatkan beberapa dokumen yang diterapkan, diantaranya dokumen prosedur daily closing, prosedur void, item correct & price override, prosedur diskon bertingkat di POS register, serta prosedur *User* ID dan *password* POS. PT Matahari Department Store belum mempunyai dokumen tersendiri mengenai manajemen risiko TI, sehingga acuan untuk manajemen risiko TI berpacu pada dokumen tersebut.

Untuk dokumen risiko TI sendiri juga belum tersedia secara lengkap dan detail, yang sudah terdokumentasi lengkap adalah risiko bisnis secara umum yang tertera pada dokumen *contingency plan* yang bersifat rahasia. Dikarenakan belum adanya dokumen risiko TI secara legal dan detail, sehingga untuk proses transaksi terkontrol dari sistem penjualan Alphapos versi manajerial. Pentingnya TI dalam perusahaan adalah untuk mengolah data administratif dan keuangan serta data persediaan setiap produk tersimpan dalam database yang dikontrol oleh sistem, sehingga pada Matahari Department Store cabang Malang Town Square sudah menggunakan sistem yang terintegrasi untuk keseluruhan department.

4.2. Wawancara

Wawancara dilakukan untuk mengetahui ruang lingkulingkup sistem. Dalam tahap ini, batas-batas sistem TI teridentifikasi, bersama dengan sumber dan informasi sistem. Dalam tahap ini terbagi atas 2 bagian yaitu:

1. Menjelaskan informasi terkait sistem yang digunakan untuk mengkarakterisasi sistem TI dan lingkungan operasional sistem
2. Mengumpulkan informasi yang relevan dengan lingkungan pemrosesan TI
3. Pada tahap ini penulis menggunakan metode *on-site interviews*dengan narasumber menggunakan daftar pertanyaan sebagai berikut:

Tabel 4. 1 Daftar pertanyaan untuk identifikasi karakteristik sistem

No	Pertanyaan	Tujuan Pertanyaan
1	Apa saja *hardware* yang digunakan untuk menunjang penggunaan sistem penjualan Alphapos?	Untuk mengetahui kebutuhan fungsional sistem IT

Tabel 4. 2 Daftar pertanyaan untuk identifikasi karakteristik sistem (lanjutan)

No	Pertanyaan	Tujuan Pertanyaan
2	Apa saja *software* yang digunakan untuk menunjang penggunaan sistem penjualan Alphapos?	Untuk mengetahui kebutuhan fungsional sistem IT
3	Bagaimana tampilan antarmuka sistem untuk konektivitas internal dan eksternal?	Untuk mengetahui arus informasi yang berkaitan dengan sistem TI
4	Apa saja data dan informasi yang diperlukan dan yang dihasilkan?	
5	Bagaimana arus informasi yang berkatian dengan sistem penjualan Alphapos	
6	Siapa saja orang yang mendukung dan menggunakan sistem IT?	Untuk mengetahui pengguna sistem
7	Apa tujuan penggunaan sistem penjualan Alphapos di Matahari?	Untuk mengetahui kebijakan keamanan yang mengatur sistem TI
8	Bagaimana kontrol operasional untuk keamnan sistem penjualan Alphapos mengenai hak istimewa untuk akses?	
9	Bagaimana keamanan lingkungan yang diterapkan untuk pemrosesan sistem penjualan Alphapos?	
10	Seberapa pentingkah sistem penjualan Alphapos dan data yang dihasilkan dalam perusahaan?	Untuk mengetahui perlindungan penyimpanan informasi yang melindungi sistem dan ketersediaan data
11	Bagaimana perlindungan penyimpanan informasi yang melidungi sistem penjualan Alphapos?	
12	Bagaimana tingkat kerentanan sistem penjualan Alphapos dan data yang dihasilkan dalam perusahaan?	Untuk mengetahui kontrol teknis, manajemen, dan operasional yang digunakan untuk sistem TI
13	Apa saja persyaratan fungsional sistem penjualan Alphapos?	
14	Kebijakan apa saja yang berlaku untuk keamanan sistem penjualan Alphapos?	
15	Bagaimana arsitektur keamanan sistem penjualan Alphapos?	Untuk mengetahui arsitektur topologi jaringan saat ini
16	Bagaimana topologi jaringan sistem penjualan Alphapos?	

Untuk detail lebih lengkap mengenai identifikasi karakteristik sistem dilampirkan pada lampiran 1 dan 2. Selanjutnya dilanjutkan dengan wawancara mengenai sumber ancaman dan bentuk ancaman. Tujuan dari langkah ini adalah untuk mengidentifikasi potensi-potensi sumber ancaman dan menyusun sebuah pernyataan daftar sumber ancaman potensial terhadap sistem TI yang dievaluasi.

Pada tahap ini dilakukan dalam bentuk wawancara langsung kepada pengguna sistem sehingga dapat lebih memahami mengenai detail sistem TI.

Tabel 4. 3 Daftar ancaman pada sistem penjualan Alphapos

No	Risk Issue
1	Pencurian perangkat
2	*Human error* (kesalahan dalam mengoperasikan sistem)
3	Akses tidak sah
4	Kebocoran data atau informasi internal perusahaan
5	Data dan informasi tidak sesuai fakta
6	Kelalaian dalam memasukan data
7	Kurangnya SDM
8	Kegagalan atau kerusakan hardware
9	*Server down*
10	*Over heat*
11	Koneksi yang tiba-tiba *offline*
12	*Over capacity*
13	*Over load*
14	Sistem error
15	Virus
16	Data korup
17	*Backup failure*

Setelah mengetahui sumber ancaman, maka selanjutnya dilaksanakan wawancara mengenai celah pada sistem penjualan Alphapos atau potensial kelemahan sistem. Tujuan dari tahap ini adalah untuk mengembangkan daftar kelemahan sistem yang dapat dieksploitasi oleh sumber ancaman.

Data yang dikumpulkan dalam tahap ini meliputi kelemahan sistem, sumber ancaman, dan penanganan ancaman tersebut. Pada tahap ini juga dilakukan *checklist* mengenai daftar pemeriksaan persyaratan keamanan yang dapat digunakan untuk mengevaluasi dan mengidentifikasi kelemahan aset, prosedur, proses, dan transfer informasi yang tidak terarah terkait dengan sistem TI.

Berikut hasil *checklist* untuk potensial kelemahan sistem penjualan Alphapos disajikan pada tabel 4.4

Tabel 4. 4 Checklist untuk potensial kelemahan sistem penjualan Alphapos

Security Area	Konten	Kendali yang ada	Checklist
Management Security	Penugasan tanggung jawab	Struktur organisasi (tinjau kembali gambar 2.1)	V
	Dukungan yang berkelanjutan	Adanya tim untuk memperbaiki kesalahan dalam sistem (tim EDP)	V

Tabel 4. 5 Checklist untuk potensial kelemahan sistem penjualan Alphapos (lanjutan)

Security Area	Konten	Kendali yang ada	Checklist
Management Security	Kemampuan untuk menangani insiden	eSOP manajemen risiko	V
	Pemeriksaan secara berkala terhadap kontrol keamanan	Pengendalian fasilitas fisik sistem (prosedur pemeriksaan setiap 2 minggu sekali)	V
	Pemeriksaan latar belakang personil	Profil setiap personil (adanya file setiap pegawai di bagian HRD)	V
	Penilaian risiko	Daftar risiko	X
	Pelatihan kemananan dan teknis	Simulasi keamanan dan teknis (adanya kartu simulasi keamanan)	V
	Sistem otorisasi	Otorisasi setiap akun (penggunaan *User* id dan *password*)	V
Operational Security	Pengendalian polusi yang ada di udara (asap, debu,dll)	Penggunaan AHU	V
	Kontrol untuk memastikan daya listrik	Penggunaan UPS central	V
	Akses dan pembuangan media data	Data berusia >60 hari otomatis terhapus oleh sistem	V
	Distribusi dan pelabelan komponen sistem	Serial number setiap komponen	V
	Perlindungan fasilitas (Ruang komputer, pusat data)	Pemberian fasilitas seperti APAR, AC, AHU	V
	Kontrol kelembaban	Penggunaan AC	V
	Pengatur suhu	Penggunaan AC	V
	Workstation, laptop, dan komputer pribadi yang berdiri sendiri	Penggunaan akun personal yang telah di sahkan oleh pusat	V
Technical Security	Komunikasi (*dial-in,* interkoneksi sistem, router)	Penggunaan HT dan dial-in	V
	Deteksi gangguan	Kontrol teknis	V
	Audit sistem	Audit internal perusahaan	V

Dari beberapa sumber ancaman dan celah yang terdapat pada sistem penjualan Alphapos, hingga kini perusahaan juga telah melaksanakan pengendalian ancaman. Maka dilaksanakan wawancara mengenai pengendalian ancaman apa saja yang sudah ada di perusahaan. Tujuan dari langkah ini adalah untuk menganalisis kontrol yang telah direncanakan dan dilaksanakan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan ancaman menggunakan kelemahan sistem.

Daftar periksa persyaratan keamanan yang sebelumnya sudah didapatkan digunakan untuk memvalidasi ketidakpatuhan keamanan dan juga pemenuhan keamanan. Output *list control* pada tahap ini digunakan untuk mengurangi adanya kerentanan pada sistem dan mengurangi dampak dari insiden risiko. Untuk lebih lengkap dokumen kontrol akan dilampirkan pada lampiran 3, lampiran 4, lampiran 5, serta lampiran 6.

Tabel 4. 6 Checklist daftar pengendalian yang diterapkan di Matahari Department Store

Kontrol	Dokumen Pendukung	Checklist
Kontrol mekanisme akses sistem	Penggunaan *password* untuk otorisasi sistem	V
Kontrol mekanisme identifikasi dan otentifikasi	Penggunaan ID *User*name dan *password* yang berbeda setiap pegawai	V
Kontrol keamanan	Prosedur *User* ID dan *Password*	V
Kontrol prosedur operasional	Prosedur daily closing, prosedur diskon bertingkat di POS register	V
Kontrol personil pengoperasi	Prosedur pengendalian POS aktif	X
Kontrol terhadap peralatan	Prosedur pelaporan komponen	V
Kontrol penyimpanan arsip	Penghapusan otomatis data berusia > 60 hari	V
Kontrol pengembangan dan pengendalian sistem	Prosedur pengembangan sistem penjualan	X
Kontrol virus	Prosedur pengendalian *software*	X
Kontrol proteksi fisik terhadap pusat data	Prosedur pengendalian lingkungan server	V
Kontrol perangkat keras	Pelaporan bulanan setiap serial number komponen	V

Untuk mendapatkan peringkat *likelihood* ditentukan oleh kemampuan sumber ancaman, sifat kerentanan, serta efektivitas kontrol yang ada saat ini. Untuk mempermudah dalam tahapan ini berikut tabel peringkat *likelihood.*

Tabel 4. 7 Peringkat *likelihood*

Rating likelihood	Kriteria *likelihood*	Definisi *likelihood*	Frekuensi
A	Tinggi	Sumber ancaman memiliki motivasi dan kemampuan namun kontrol yang ada tidak efektif untuk mencegah ancaman	>10 kali dalam 1 bulan
B	Sedang	Sumber ancaman memiliki motivasi dan kemampuan namun kontrol yang ada mampu untuk menghambat ancaman	6-10 kali dalam 1 bulan
C	Rendah	Sumber ancaman tidak memiliki motivasi atau kemampuan atau kontrol yang ada mampu untuk menghalangi ancaman	0-5 kali dalam 1 bulan

Berikut hasil analisis peringkat *likelihood* dari setiap sumber ancaman yang selanjutnya dikonversikan kedalam kategori rendah, sedang, ataupun tinggi.

Tabel 4. 8 Hasil peringkat *likelihood* risiko

No	Kategori Aset	Risk Issue	Frekuensi terjadi dalam 1 Bulan	Level *likelihood*
1	Personil	Pencurian perangkat	0	Rendah
2		*Human error* (kesalahan dalam mengoperasikan sistem)	8	Sedang
3		Akses tidak sah	40	Tinggi
4		Kebocoran data atau informasi internal perusahaan	0	Rendah
5		Data dan informasi tidak sesuai fakta	4	Rendah
6		Kelalaian dalam memasukan data	4	Rendah

Tabel 4. 9 Hasil peringkat *likelihood* risiko (lanjutan)

No	Kategori Aset	Risk Issue	Frekuensi terjadi dalam 1 Bulan	Level *likelihood*
7		Kurangnya SDM	0	Rendah
8	Perangkat Keras	Kegagalan atau kerusakan hardware	4	Rendah
9		*Server down*	0	Rendah
10		*Over heat*	2	Rendah
11		Koneksi yang tiba-tiba *offline*	12	Tinggi
12		*Over capacity*	0	Rendah
13		*Over load*	0	Rendah
14	Perangkat lunak	Sistem error	4	Rendah
15		Virus	2	Rendah
16	Informasi	Data korup	1	Rendah
17		*Backup failure*	1	Rendah

Pengaruh ancaman atau dampak ancaman digunakan untuk mengetahui dampak buruk yang diakibatkan sebuah ancaman yang berhasil melakukan risiko. Dalam pemeringkatannya dikaitkan dengan prioritas informasi organisasi yang sensitif dan aset kritis seperti perangkat keras, perangkat lunak, sistem, layanan, dan aset teknologi terkait yang mendukung misi organisasi.

Untuk mempermudah dalam tahapan ini maka disajikan pada tabel 4.10

Tabel 4. 10 Skala dampak sumber risiko

Sebutan	Uraian	Peringkat
Tinggi	Semua sasaran tidak dapat tercapai	I
Sedang	Mempengaruhi pencapaian beberapa sasaran	II
Rendah	Dampak kecil terhadap sasaran yang dapat diabaikan	III

Hasil dari tahap ini adalah *magnitude of impact* seperti yang disajikan dalam tabel 4.11

Tabel 4. 11 *Magnitude of impact*

No	Kategori Aset	Risk Issue	*Magnitude of impact*
1		Pencurian perangkat	Tinggi
2		*Human error* (kesalahan dalam mengoperasikan sistem)	Sedang
3		Akses tidak sah	Tinggi
4		Kebocoran data atau informasi internal perusahaan	Tinggi
5		Data dan informasi tidak sesuai fakta	Sedang
6		Kelalaian dalam memasukan data	Sedang
7		Kurangnya SDM	Sedang
8	Perangkat Keras	Kegagalan atau kerusakan hardware	Tinggi
9		*Server down*	Tinggi
10		*Over heat*	Sedang
11		Koneksi yang tiba-tiba *offline*	Tinggi
12		*Over capacity*	Sedang
13		*Over load*	Tinggi
14	Perangkat lunak	Sistem error	Tinggi
15		Virus	Tinggi
16	Informasi	Data korup	Sedang
17		*Backup failure*	Tinggi

BAB 5 ANALISIS

5.1. Analisis Karakter Sistem

Hasil wawancara menunjukan bahwa sistem penjualan Alphapos memiliki peranan yang sangat penting dalam perusahaan yang digunakan untuk proses transaksi dan inventori barang pada perusahaan. Sistem penjualan Alphapos ini digunakan untuk menghimpun, menyimpan, dan memproses data transaksi serta kadangkala mengendalikan keputusan yang merupakan bagian dari transaksi. Hal ini menunjukkan bahwa sistem penjualan Alphapos digunakan sebagai *transaction processing system* (TPS). Hal ini dibuktikan bahwa sistem penjualan Alphapos mengelola data yang besar, menggunakan rumus komputasi yang sederhana, dan dilakukan secara rutin.

Pada penggunaan sistem penjualan Alphapos mendukung pemakaian beberapa buah komputer yang terhubung dalam jaringan komputer, pada Matahari jaringan yang digunakan adalah intranet dan internet. Internet digunakan untuk melakukan sinkronisasi data antara server pusat dengan server toko, sedangkan intranet digunakan untuk mendukung dalam penggunaan sistem di lingkungan toko.

Pada penggunaan sistem penjualan Alphapos di Matahari terdapat dua jenis, yaitu server untuk bagian manajerial serta *client* untuk kasir. Terdapat beberapa perangkat keras yang dibutuhkan untuk mengimplementasikan sistem penjualan Alphapos diantaranya CPU, Customer display, Printer, Monitor, Keyboard, Cash drawer, Scanner, dan Kabel UTP/WiFi.

Gambar 5. 1 Perangkat keras yang dibutuhkan sistem penjualan Alphapos

Rincian fungsi dari setiap komponen POS Register, diantaranya:

1. Scanner, berfungsi untuk membaca kode barcode dari suatu barang sehingga dapat membantu menginputkan data barang yang akan dijual.
2. Printer, berfungsi untuk mencetak struk atau bukti transaksi penjualan.
3. Drawer, berfungsi untuk menyimpan uang yang berada pada meja kasir.
4. Customer display, berfungsi untuk menunjukkan kepada pelanggan tentang barang apa saja yang dibeli, jumlah transaksi, uang kembalian dan lain sebagainya.
5. Keyboard, berfungsi untuk menginput jumlah barang, diskon, dan lain sebagainya.
6. Monitor, berfungsi untuk menunjukkan kepada *User* mengenai detail transaksi.
7. CPU, berfungsi untuk menjalankan sistem operasi dan sistem penjualan.

Terdapat tiga menu inti pada sistem penjualan Alphapos. Yang pertama Report Sales, Report ini digunakan untuk menyajikan report penjualan perjamnya dan jangka waktu hari. Report sales bisa diakses mulai dari penjualan by item (perSKU), penjualan by brand, penjualan by dept (penggabungan sesuai kategori brand), dan penjualan by world (Ladies, Intimate, bag accecories, Beauy, Children, Youth Girl, Youth boy, Men's, Home, Shoes). Yang kedua adalah Database Processing, menu Database Processing digunakan untuk upload data manual (Struk Kupon Diskon, Upload database manual) dan juga terdapat menu EoD (end of day) yang hanya bisa dilakukan oleh role *Auxilary* dan *Manager*. Yang ketiga adalah Database Log, menu ini menyajikan data history *User* Alphapos, menu ini berguna untuk memantau jika ada error pada server yang diakibatkan oleh human error (kesalahan dalam mengoperasikan sistem) serta untuk mengetahui aktivitas-aktivitas yang dilakukan oleh setiap mesin POS. Dengan terdapatnya fitur ini dapat memudahkan pihak manajemen untuk memantau transaksi mana yang mencurigakan.

Kelompok pengguna pada sistem penjualan Alphapos dibagi menjadi empat menurut role otorisasinya, yaitu:

a. *Auxilary*: Bisa mengakses, edit, upload seluruh database pada Software Alphapos. Role ini hanya bisa digunakan oleh Store *Manager* dan Assistant *Manager*.
b. *Manager*: Bisa mengakses dan hanya upload database pada Software Alphapos. Role ini hanya berlaku untuk Supervisor , Koordinator dan EDP (*Entry Data Proccesor*)
c. *Expedition*: Bisa akses data Alphapos dan Software penerimaan barang digunakan oleh tim Ekspedisi.

d. *User*: Hanya untuk akses report data dan tidak bisa upload atau edit data. Role ini digunakan oleh kasir dan pramuniaga

Pada saat ini terdapat beberapa peraturan yang sudah diterapkan untuk keamanan sistem penjualan Alphapos. Yang pertama role otorisasi, dengan adanya role otorisasi tidak semua karyawan bisa mengakses hal yang beresiko, misal edit database Alphapos hanya bisa dilakukan oleh role *Auxilary* saja. Yang kedua aturan untuk *User* ID, *User* ID tiap karyawan matahari berbeda satu dengan yang lainnya. Sehingga *User* satu tidak bisa menggunakan *User* lain. Yang ketiga, setiap aplikasi memiliki *password* aplikasi yang mana setiap aplikasi yang digunakan diproteksi dengan *password* dan ID yang berbeda. Sehingga faktor keamanan lebih terjamin. Yang keempat usia *password*, setiap *password* dan *User* ID dan aplikasi harus diganti secara berkala selama 60 hari, Jika tidak *password* akan expired dan dibutuhkan role *Auxilary* untuk update *password*.

5.2. Analisis Ancaman dan Celah pada Sistem penjualan Alphapos

Pada dasarnya risiko akan terjadi apabila terdapat ancaman dan celah pada suatu sistem. Dari hasil wawancara menunjukkan beberapa ancaman dan celah pada sistem penjualan Alphapos. Bentuk ancaman yang terjadi dikelompokkan bedasarkan empat kategori aset, yaitu personil, perangkat keras, perangkat lunak, dan informasi. Ancaman yang ada pada sistem penjualan Alphapos akan ditabulasikan pada tabel 5.1

Tabel 5. 1 Ancaman pada sistem penjualan Alphapos

No	Kategori Aset	Risk Issue
1	Personil	Pencurian perangkat
2		*Human error* (kesalahan dalam mengoperasikan sistem)
3		Akses tidak sah
4		Kebocoran data atau informasi internal perusahaan
5		Data dan informasi tidak sesuai fakta
6		Kelalaian dalam memasukan data
7		Kurangnya SDM
8	Perangkat Keras	Kegagalan atau kerusakan hardware
9		*Server down*
10		*Over heat*
11		Koneksi yang tiba-tiba *offline*
12		*Over capacity*
13		*Over load*
14	Perangkat lunak	Sistem error
15		Virus
16	Informasi	Data korup
17		*Backup failure*

Untuk kelemahan dari sistem penjualan Alphapos, belum terdapatnya dokumen mengenai daftar risiko spesifik mengenai sistem IT yang ada. Sehingga diperlukan dokumentasi mengenai risiko yang ada pada sistem IT atau sistem penjualan Alphapos.

BAB 6 PEMBAHASAN

6.1. Daftar Risiko

Pada sistem informasi kategori aset dibagi menjadi 4 bagian yaitu personil, perangkat keras, perangkat lunak, dan informasi. Pada tabel 6.1 menjelaskan mengenai rekapitulasi risiko berdasarkan kategori aset kemudian dikonversikan kedalam bentuk presentase. Dari pengumpulan data menghasilkan bahwa presentase *risk issue* tertinggi ditunjukan oleh kategori aset personil dengan nilai 41,18%.

Tabel 6. 1 Rekapitulasi Risiko Berdasarkan Kategori Aset

No	Kategori Aset	Jumlah *Risk Issue*	Presentase (%)
1	Personil	7	41,18
2	Perangkat Keras	6	35,30
3	Perangkat Lunak	2	11,76
4	Informasi	2	11,76
Total		17	100,00

6.2. Peringkat Risiko

Dari peringkat risiko yang dihasilkan dapat menggambarkan dampak risiko yang terdapat pada proses kerja. Untuk menentukan nilai pada matriks peringkat risiko ditentukan dengan hasil perkalian antara *magnitude of impact* dengan level *likelihood*. Pada tabel 6.2 ditampilkan mengenai matrik peringkat risiko dengan penilaian rendah, sedang, dan tinggi. Dimana penentuan deskripsi *risk level* sesuai dengan tabel 2.2 yang menjelaskan risiko dikatakan tinggi apabila memiliki nilai >50 hingga 100, untuk risiko dikatakan sedang apabila memiliki nilai >10 hingga 50, sedangkan untuk risiko yang dikatakan rendah apabila memiliki nilai 1 hingga 10.

Tabel 6. 2 Penilaian Risiko

No	Kategori Aset	Risk Issue	Level *likelihood*	*Magnitude of impact*	*Risk level*	Deskripsi *Risk Level*
1	Personil	Pencurian perangkat	Rendah (0,1)	Tinggi (100)	10	Rendah
2		*Human error* (kesalahan dalam mengoperasikan sistem)	Sedang (0,5)	Sedang (50)	25	Sedang

Tabel 6. 3 Penilaian Risiko (lanjutan)

No	Kategori Aset	Risk Issue	Level *likelihood*	*Magnitude of impact*	*Risk level*	Deskripsi *Risk Level*
3	Personil	Akses tidak sah	Tinggi (1,0)	Tinggi (100)	100	Tinggi
4		Kebocoran data atau informasi internal perusahaan	Rendah (0,1)	Tinggi (100)	10	Rendah
5		Data dan informasi tidak sesuai fakta	Rendah (0,1)	Sedang (50)	5	Rendah
6		Kelalaian dalam memasukan data	Rendah (0,1)	Sedang (50)	5	Rendah
7		Kurangnya SDM	Rendah (0,1)	Sedang (50)	5	Rendah
8	Perangkat Keras	Kegagalan atau kerusakan hardware	Rendah (0,1)	Tinggi (100)	10	Rendah
9		*Server down*	Rendah (0,1)	Tinggi (100)	10	Rendah
10		*Over heat*	Rendah (0,1)	Sedang (50)	5	Rendah
11		Koneksi yang tiba-tiba *offline*	Tinggi (1,0)	Tinggi (100)	100	Tinggi
12		*Over capacity*	Rendah (0,1)	Sedang (50)	5	Rendah
13		*Over load*	Rendah (0,1)	Tinggi (100)	10	Rendah
14	Perangkat lunak	Sistem error	Rendah (0,1)	Tinggi (100)	10	Rendah
15		Virus	Rendah (0,1)	Tinggi (100)	10	Rendah
16	Informasi	Data korup	Rendah (0,1)	Sedang (50)	5	Rendah
17		*Backup failure*	Rendah (0,1)	Tinggi (100)	10	Rendah

Dari hasil penilaian perkalian antara tingkat *likelihood* dengan *magnitude of impact* akan menentukan nilai risiko yang dihasilkan dari setiap *risk issue*. Yang mana hasil tersebut diperingkatkan pada tabel 6.4

Tabel 6. 4 Hasil peringkat risiko sistem penjualan Alphapos

No	Kategori Aset	Risk Issue	Level *likelihood*	*Magnitude of impact*	*Risk level*	Deskripsi *Risk Level*
1	Personil	Akses tidak sah	Tinggi (1,0)	Tinggi (100)	100	Tinggi
2	Perangkat Keras	Koneksi yang tiba-tiba *offline*	Tinggi (1,0)	Tinggi (100)	100	Tinggi
3	Personil	*Human error* (kesalahan dalam mengoperasikan sistem)	Sedang (0,5)	Sedang (50)	25	Sedang
4	Personil	Pencurian perangkat	Rendah (0,1)	Tinggi (100)	10	Rendah
5	Personil	Kebocoran data atau informasi internal perusahaan	Rendah (0,1)	Tinggi (100)	10	Rendah
6	Perangkat Keras	Kegagalan atau kerusakan hardware	Rendah (0,1)	Tinggi (100)	10	Rendah
7	Perangkat Keras	*Server down*	Rendah (0,1)	Tinggi (100)	10	Rendah
8	Perangkat Keras	*Over load*	Rendah (0,1)	Tinggi (100)	10	Rendah
9	Perangkat lunak	Sistem error	Rendah (0,1)	Tinggi (100)	10	Rendah
10	Perangkat lunak	Virus	Rendah (0,1)	Tinggi (100)	10	Rendah
11	Informasi	*Backup failure*	Rendah (0,1)	Tinggi (100)	10	Rendah
12	Personil	Data dan informasi tidak sesuai fakta	Rendah (0,1)	Sedang (50)	5	Rendah
13	Personil	Kelalaian dalam memasukan data	Rendah (0,1)	Sedang (50)	5	Rendah
14	Perangkat Keras	Kurangnya SDM	Rendah (0,1)	Sedang (50)	5	Rendah

Tabel 6. 5 Hasil peringkat risiko sistem penjualan Alphapos (lanjutan)

No	Kategori Aset	Risk Issue	Level *likelihood*	*Magnitude of impact*	*Risk level*	Deskripsi *Risk Level*
15	Perangkat Keras	*Over heat*	Rendah (0,1)	Sedang (50)	5	Rendah
16	Perangkat Keras	*Over capacity*	Rendah (0,1)	Sedang (50)	5	Rendah
17	Informasi	Data korup	Rendah (0,1)	Sedang (50)	5	Rendah

Dari hasil penilaian risiko maka dilakukan rekapitulasi nilai risiko bedasarkan kategori aset seperti pada tabel 6.6 yang menghasilkan risiko dengan nilai sedang terdapat pada kategori aset personil dan perangkat keras, yang selanjutnya menjadi TOP IT Risk yang akan diberikan rekomendasi pengendalian.

Tabel 6. 6 Rekapitulasi Nilai Risiko Bedasarkan Kategori Aset

No	Kategori Aset	Nilai Risiko		
		Rendah	Sedang	Tinggi
1	Personil	5	1	1
2	Perangkat Keras	5	0	1
3	Perangkat Lunak	2	0	0
4	Informasi	2	0	0
Total		14	1	2

6.3. Top IT Risk

Dari 17 *risk issue* yang telah dijabarkan difokuskan pada top IT risk untuk diberikan rekomendasi pengendalian dari setiap risiko. Risiko tersebut dari kategori aset personil dengan rincian *Human error* (kesalahan dalam mengoperasikan sistem), serta Akses tidak sah merupakan risiko yang paling sering terjadi mengingat otorisasi digunakan untuk memberikan diskon lebih dari 70% yang diinputkan secara manual. Untuk kategori aset perangkat keras dengan risk issue koneksi yang tiba-tiba *offline* sehingga menyebabkan terhambatnya pemantauan transaksi secara langsung.

6.4. Rekomendasi Pengendalian Risiko

Setelah ditentukan *Top IT Risk* dari perusahaan maka selanjutnya adalah memberikan rekomendasi pengendalian risiko pada setiap bentuk risiko yang

mungkin terjadi. Rekomendasi yang diberikan bedasarkan dari beberapa literatur disajikan pada tabel 6.7

Tabel 6. 7 Opsi rekomendasi pengendalian risiko

Kategori Aset	*Risk Issue*	Opsi Rekomendasi Pengendalian	Jenis Pengendalian Risiko
Personil	*Human error* (kesalahan dalam mengoperasikan sistem)	1. Memberikan pelatihan yang tepat	Risk reduction
	Akses tidak sah	1. Diberlakukan format khusus dalam pembuatan *password*	Risk avoidance
		2. Dibutuhkan peran admin dalam memonitor *log login* sistem aplikasi	Risk reduction
Perangkat Keras	Koneksi yang tiba-tiba *offline*	1. Mengontrol jaringan dengan cara dimonitoring	Risk reduction
		2. Memelihara keamanan sistem dengan ditinjau secara berkala	Risk reduction

6.5 Mitigasi Risiko

Pada mitigasi risiko akan diberikan rekomendasi pengendalian risiko yang tepat pada setiap risiko yang diprioritaskan pada bagian sebelumnya dan dibandingkan dengan setiap pilihan mitigasi risiko yang ada untuk memperoleh keuntungan yang besar dan meminimalisir risiko yang ada. Untuk mengetahui detail setiap pilihan maka digunakan *cost benefit analysis* dengan menganalisa dampak apabila digunakan rekomendasi pengendalian serta apabila tidak digunakan rekomendasi pengendalian.

6.5.1 Human error (kesalahan dalam mengoperasikan sistem)

Untuk membantu menentukan mitigasi risiko yang tepat maka digunakan opsi rekomendasi pengendalian yang sebelumnya telah dijelaskan pada tabel 5.4 untuk risiko *human error* (kesalahan dalam mengoperasikan sistem). Yang selanjutnya akan dilakukan *cost benefit analysis* untuk setiap opsi rekomendasi pengendalian untuk menentukan prioritas mitigasi risiko.

1. Memberikan pelatihan yang tepat
   Pada risiko *human error* seperti kesalahan memasukan data yang disebabkan oleh kelalaian pegawai yang mana ditunjang dengan

kurangnya pelatihan atau training karyawan secara berkala maka pilihan pengendalian risiko yang tepat adalah dengan memberikan pelatihan yang tepat.

Dampak apabila pemberian pelatihan dilakukan adalah meningkatnya produktivitas pegawai seiring dengan meningkatnya pemahaman mengenai pengoperasian sistem. Sehingga tidak banyak waktu terbuang hanya untuk memperbaiki kesalahan dalam mengoperasikan sistem.

Sedangkan apabila tidak diberikan pelatihan maka akan berdampak tidak banyak biaya yang keluar untuk memberikan pelatihan. Namun akan banyak waktu yang terbuang hanya untuk memperbaiki kesalahan. Hal tersebut berujung dengan menurunnya produktivitas kerja pegawai dan tidak tercapainya target penjualan dari perusahaan.

Tabel 6. 8 Perhitungan Cost untuk memberikan pelatihan yang tepat

	Jumlah individu	Harga per individu	Total
Biaya pelatihan	24	Rp 3.500.000	Rp 84.000.000
Transportasi rata-rata	24	Rp 100.000	Rp 2.400.000
Lumpsum rata-rata	24	Rp 1.500.000	Rp 36.000.000
Total			Rp 122.400.000

Benefit

Mengurangi kesalahan (seperti : waktu yang hilang untuk memperbaiki kesalahan)

Mereduksi durasi transaksi

Dari hasil *cost benefit analysis* tersebut maka direkomendasikan untuk memberikan pelatihan yang tepat dan merupakan *risk reduction.* Dalam perusahaan PT Matahari Department Store pelatihan yang dimaksud adalah *training* peningkatan kinerja pegawai.

6.5.2 Akses tidak sah

Dalam mengendalikan risiko pencurian *password* maka dapat diatasi dengan dua opsi pengendalian risiko diantaranya diberlakukan format khusus dalam pembuatan *password* dan dibutuhkan peran admin dalam memonitor *log login* sistem aplikasi. Untuk memprioritaskan pengendalian risiko yang dipilih maka dibantu dengan pemaparan menggunakan *cost benefit analysis* sebagai berikut

1. Diberlakukan format khusus dalam pembuatan *password*
   Dampak apabila diberlakukan format khusus dalam pembuatan *password* adalah tidak mudahnya untuk dicuri oleh pihak lain, karena standar keamanan dalam menyusun format khusus akan dibuat lebih rumit.
   Dampak apabila tidak diberlakukannya rekomendasi pengendalian ini adalah akan tetap ada pencurian *password* oleh pihak tertentu dikarenakan *password* yang ada tidak terlalu rumit sehingga mudah untuk dihafalkan oleh pihak lain dan disalahgunakan untuk kepentingan pribadi.

   Cost
   -

   Benefit
   Mengurangi tindak pencurian *password*
   Meningkatkan standar keamanan setiap akun
   Memperkecil *opportunity loss*

2. Memonitor *log login* sistem aplikasi dengan bantuan peran admin
   Dampak apabila memonitor *log* sistem dengan bantuan peran admin, akan terlihat transaksi-transaksi yang tidak wajar. Sehingga dapat dilacak lebih awal, dan di selesaikan lebih awal. Akan berdampak pula pada penurunan kerugian yang ditanggung perusahaan akibat penggunaan otorisasi untuk kepentingan pribadi.
   Dampak apabila tidak adanya monitor *log* sistem, maka tindak penggunaan otorisasi secara tidak wajar tidak akan terlacak dan perusahaan akan menerima kerugian seperti kehilangan barang dan keuangan.

Tabel 6. 9 Perhitungan cost bantuan admin

	Jumlah individu	Harga per individu	Total
Gaji admin	1	Rp 2.400.000	Rp 2.400.000
Total			Rp 2.400.000

Benefit
Mengurangi kesalahan (seperti : jumlah transaksi yang salah mencurigakan)
Memperkecil *opportunity loss*

Dari hasil *cost benefit analysis* tersebut maka diprioritaskan untuk memberikan format khusus dalam pembuatan *password* yang merupakan *risk avoidance.* Lalu memonitor *log login* sistem aplikasi dengan bantuan peran admin yang merupakan *risk reduction*.

6.5.3 Koneksi yang tiba-tiba *offline*

Dalam mengendalikan risiko koneksi yang tiba-tiba *offline* maka dapat diatasi dengan dua opsi pengendalian risiko diantaranya mengontrol jaringan dengan cara dimonitoring dan memelihara keamanan sistem dengan ditinjau secara berkala. Untuk memprioritaskan pengendalian risiko yang dipilih maka dibantu dengan pemaparan menggunakan *cost benefit analysis* sebagai berikut

1. Mengontrol jaringan dengan cara dimonitoring
   Dampak apabila mengontrol jaringan dilaksanakan adalah akan terdeteksi lebih awal apabila jaringan mengalami gangguan. Sehingga tidak terjadi hambatan dalam penggunaan sistem dan durasi transaksi tidak akan lama.
   Dampak apabila tidak dilaksanakan maka ketika terjadi gangguan pada jaringan tidak akan terdeteksi dan akan menghambat dalam melakukan transaksi, sehingga durasi transaksi menjadi lama.

   Cost
   -
   Benefit
   Mengurangi kesalahan (seperti : waktu yang hilang untuk memperbaiki kesalahan)
   Mereduksi durasi transaksi karena *respond time* dari sistem yang cepat
   Dengan kontrol yang rutin dapat mencegah koneksi yang tidak stabil

2. Memelihara keamanan sistem dengan ditinjau secara berkala
   Dampak apabila memelihara keamanan sistem maka akan mencegah kerusakan pada sistem yang menyebabkan sistem tidak bisa terhubung ke jaringan. Sehingga proses backup dan pelaporan transaksi dapat berjalan lancer.
   Sedangkan apabila tidak dilaksanakan maka akan berakibat sistem tidak dapat digunakan karena tidak dapat terhubung ke jaringan.

   Cost
   -
   Benefit
   Mengurangi kesalahan (seperti : waktu yang hilang untuk memperbaiki kesalahan)
   Mereduksi durasi transaksi karena *respon time* dari sistem yang cepat

Dari hasil *cost benefit analysis* tersebut maka dimungkinkan untuk dilaksanakan bersamaan pengendalian risiko mengontrol jaringan dengan cara dimonitoring dan memelihara keamanan sistem dengan ditinjau secara berkala yang keduanya termasuk dalam *risk reduction.*

BAB 7 PENUTUP

7.1 Kesimpulan

Dalam melakukan analisis risiko teknologi informasi sesuai dengan ISO 31000 dimulai dari karakterisasi sistem agar mengetahui komponen apa saja yang dibutuhkan untuk menggunakan sistem penjualan Alphapos. Lalu mengidentifikasi ancaman serta kelemahan sistem penjualan Alphapos yang merupakan komponen dasar terjadinya risiko. Lalu menganalisis pengendalian apa saja yang telah diterapkan di perusahaan untuk mengetahui apa yang salah dari pengendalian yang sudah ada. Selanjutnya menganalisis kemungkinan risiko tersebut terjadi serta dampak yang mungkin disebabkan. Dari hasil tersebut dapat ditentukan risiko mana yang diprioritaskan dan yang harus dikendalikan.

Dengan menggunakan ISO 31000 akan terlihat risiko pada sistem penjualan Alphapos yang dapat dikategorikan kedalam tiga tingkat yaitu, tinggi, sedang, dan rendah. Dimana dari hasil penelitian menunjukan bahwa risiko yang harus diprioritaskan adalah *human error* (kesalahan dalam mengoperasikan sistem), pencurian *password*, serta tidak stabilnya koneksi dalam menjalankan sistem penjualan Alphapos.

Dari hasil mitigasi risiko yang dilakukan dibantu oleh *cost benefit analysis* maka menghasilkan *risk reduction* untuk risiko *human error* (kesalahan dalam mengoperasikan sistem)*, risk avoidance* untuk risiko Akses tidak sah, serta *risk reduction* untuk risiko koneksi yang tidak stabil.

7.2 Saran

Saran yang dapat digunakan oleh PT Matahari Dept Store cabang Malang Town Square maupun peneliti selanjutnya adalah sebagai berikut:

1. Untuk melakukan analisis risiko teknologi TI sebaiknya menggunakan *framework* yang lebih teknis.
2. Penilaian risiko yang dilakukan hanya sebatas aset TI yang mendukung proses kerja utama perusahaan, ke depan diharapkan semua aset TI dapat teridentifikasi risikonya.
3. Jika terdapat risiko TI baru yang disebabkan perkembangan TI, dapat diidentifikasi dan dikategorikan bedasarkan *framework*.

Daftar Pustaka

ACMF, n.d. *ASEAN CORPORATE GOVERNANCE SCORECARD.* [Online] Available at: http://www.theacmf.org/ACMF/upload/asean_cg_scorecard.pdf

Andrianto Moeljono, M., 2016. *Manajemen Risiko Teknologi Informasi.* [Online] Available at: https://itgid.org/manajemen-risiko-teknologi-informasi-part-i/

Indrajit, D. R. E., 2004. *Kajian Strategis Analisis Cost-Benefit Investasi Teknologi Informasi,* Yogyakarta: Penerbit Andi.

ISO, 2009. *ISO 31000 : Risk management - principles and guidelines.* Switzerland: ISO.

Kadir, A., 2014. *Pengenalan SIstem Informasi Edisi Revisi.* II ed. Yogyakarta: Andi.

Lientz, B. P. & Larssen, L., 2006. *Risk Management for IT Projects : how to deal with over 150 issues and risks.* Burlington: Elsevier Inc.

Mahersmi, B. L., Muqtadiroh, F. A. & Hidayanto, B. C., 2016. Analisis Risiko Keamanan Informasi dengan Menggunakan Metode Octave dan Kontrol ISO 27001 pada DISHUBKOMINFO Kabupaten Tulungagung. *Seminar Nasional Sistem Informasi Indonesia* , pp. 181-194.

Moningka, C., 2016. Ergonomi : Human Error dan Antisipasinya. *Buletin Konsorsium Psikologi Ilmiah Nusantara.*

Nice, F. L. & Imbar, R. V., 2016. Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000. *JUISI.*

PT Link Net Tbk, 2014. *Tata Kelola Perusahaan (GCG),* Jakarta: PT Link Net Tbk.

Redaksi, 2015. *4 Cara Memperbaiki Kesalahan Akibat Human Error.* [Online] Available at: http://shiftindonesia.com/4-cara-memperbaiki-kesalahan-akibat-human-error/

Rilyani, A. N., W, Y. F. A. & Jatmiko, D. D., 2015. Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi kasus : i-Gracias Telkom University). *e-Proceeding of Engineering,* pp. 6201-6208.

Safaat, N., 2011. Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 (Studi Kasus : Sistem Infrastruktur TI Telkom Indonesia). *Jurnal Sains, Teknologi dan Industri,* pp. 52-66.

Samaptoaji, S., 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) Pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri,* Jakarta: s.n.

Sari, W. D., Papilaya, F. S. & Manuputty, A. D., 2017. Evaluasi Pengendalian Aplikasi pada Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA). *Jurnal Sistem Informasi Indonesia (JSII) Vol 2 No 1.*

Stergiopoulos, G., Gritzalis, D. & Kouktzoglou, V., 2018. Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment. *Elsevier,* pp. 23-45.

Stonebumer, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems.* Gaithersburg: National Institute of Standards and Technology.

Susilo, L. J. & Kaho, V. R., 2017. *Manajemen Risiko berbasis ISO 31000 untuk Industri Nonperbankan.* Jakarta Pusat: PPM.

Tampubolon, A. R. & Suhardi, 2011. Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010. *Jurnal Telematika.*