MAKALAH

IKI-83408T: Proteksi dan Teknik Keamanan Sistem Informasi

PT. Asuransi XYZ

Kelompok 107

7204000187	**Trijana Pratisthitha**
7203012122	**Janus Limar**
720301222X	**Rony Baskoro Lukito**

Magister Teknologi Informasi
Fakultas Ilmu Komputer Universitas Indonesia

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

Asuransi kredit yang diselenggarakan oleh PT Asuransi XYZ, memberikan perlindungan terhadap resiko kegagalan pembayaran oleh pembeli yang mungkin terjadi dalam suatu transaksi perdagangan.

Transaksi perdagangan ternyata mengandung risiko cukup besar. Apalagi dalam sistem perdagangan modern seperti saat ini, risiko yang dihadapi oleh para pelaku bisnis bertambah. Salah satunya adalah risiko kegagalan pembayaran yang mungkin saja terjadi dalam suatu transaksi.

Dalam pasar yang kompetitif, biasanya para pelaku bisnis memasukkan penawaran kemudahan dalam hal pembayaran kepada pembeli, untuk meningkatkan daya saing. Hal yang berisiko, tetapi kemudahan pembayaran telah menjadi bagian dari daya saing dalam pasar yang kompetitif.

Sejumlah sistem pembayaran seperti sistem pembayaran berjangka atau kredit, baik dengan letter of credit (L/C) atau tanpa L/C, dengan Document Against Payment (D/P), atau Document Against Acceptance (D/A), dan konsinyasi, memiliki resiko untuk tidak dilunasi.

Risikonya, jika terjadi kegagalan pembayaran, bisa dipastikan pihak penjual akan mengalami kerugian, karena barang sudah dikirim dengan biaya mahal, uang yang ditunggu tak kunjung datang. Tetapi untunglah ada asuransi kredit yang selama ini sangat membantu para pelaku bisnis.

Beberapa risiko kegagalan yang mungkin timbul, antara lain, pembeli mengalami kebangkrutan alias pailit atau keterlambatan pembayaran karena permasalahan yang bersifat teknis perbankan.

1.2. Tujuan

Tujuan dari penulisan makalah ini adalah untuk membahas domain-domain keamanan yang ada pada perusahaan asuransi PT. XYZ. Dengan pembahasan tersebut

diharapkan dapat ditemukan permasalahan-permasalahan yang ada dan diharapkan dapat dicari solusi-solusi yang efektif dan efisien untuk menanggulanginya.

Domain-domain yang akan dibahas adalah sebelas domain keamanan yaitu:

1. Security Management Practices
2. Access Control System & Methodology
3. Telecommunications & Network Security
4. Cryptography
5. Security & Architecture Models
6. Operations Security
7. Application & System Development Security
8. Disaster Recovery & Business Continuity Plan
9. Laws, Investigations & Ethics
10. Physical Security
11. Auditing

1.3. Profil Perusahaan

PT. Asuransi XYZ didirikan pada tahun 1971, sebagai bagian dari upaya menumbuhkembangkan Usaha Kecil dan Menengah (UKM).

Pada awalnya untuk melaksanakan upaya tersebut, PT. Asuransi XYZ menjalankan usaha Asuransi Kredit Bank dan dalam perkembangan selanjutnya upaya tersebut dilengkapi dengan usaha-usaha lainnya, khususnya di bidang penjaminan. Jenis jasa yang yang baru ini tidak hanya memperbesar akses pengusaha terhadap sumber perkreditan, tetapi juga mendukung arus perdagangan di dalam dan luar negeri

Seluruh usaha tersebut, pada dasarnya memiliki manfaat yang hampir sama yaitu memperbesar akses sektor riil terhadap sektor finansial.

Dengan menjalankan usaha-usaha tersebut, PT. Asuransi XYZ mtelah membantu lebih dari 6 juta UKM dalam memperkuat struktur usahanya, terutama yang bersifat finansial

Misi

Mendukung program pemerintah di bidang ekonomi dalam menciptakan Usaha Kecil dan Menengah (UKM) yang tangguh melalui kegiatan usaha asuransi dan/atau penjaminan

Visi

Menjadi Perusahaan asuransi Nasional terpecaya dan kompetitif yang mengutamakan pelayanan prima dengan dukungan sumber daya dan lembaga keuangan yang kuat di dalam dan luar negeri untuk pihak-pihak yang berkepentingan

PRODUK

Asuransi Kredit Bank

Memberikan perlindungan kepada perbankan atas resiko kerugian akibat kredit macet, khususnya kredit yang diberikan kepada UKM

Penjaminan Kredit

Memberikan jaminan kepada UKM untuk memudahkan UKM memperoleh pembiayaan dari lembaga keuangan, khususnya dari Bank

Jasa Manajemen Kredit

Mendukung pengelolaan penjualan barang secara kredit melalui :
Memberikan saran atas kebijakan kredit yang diterapkan penjual Membantu pengelolaan tunggakan piutang Menutup kerugian akibat piutang macet

Surety Bond

memberikan jaminan yang diperlukan untuk memastikan berbagai ntahap pelaksanaan proyek dan meningkatkan kepercayaan dalam berbagi jenis transaksi

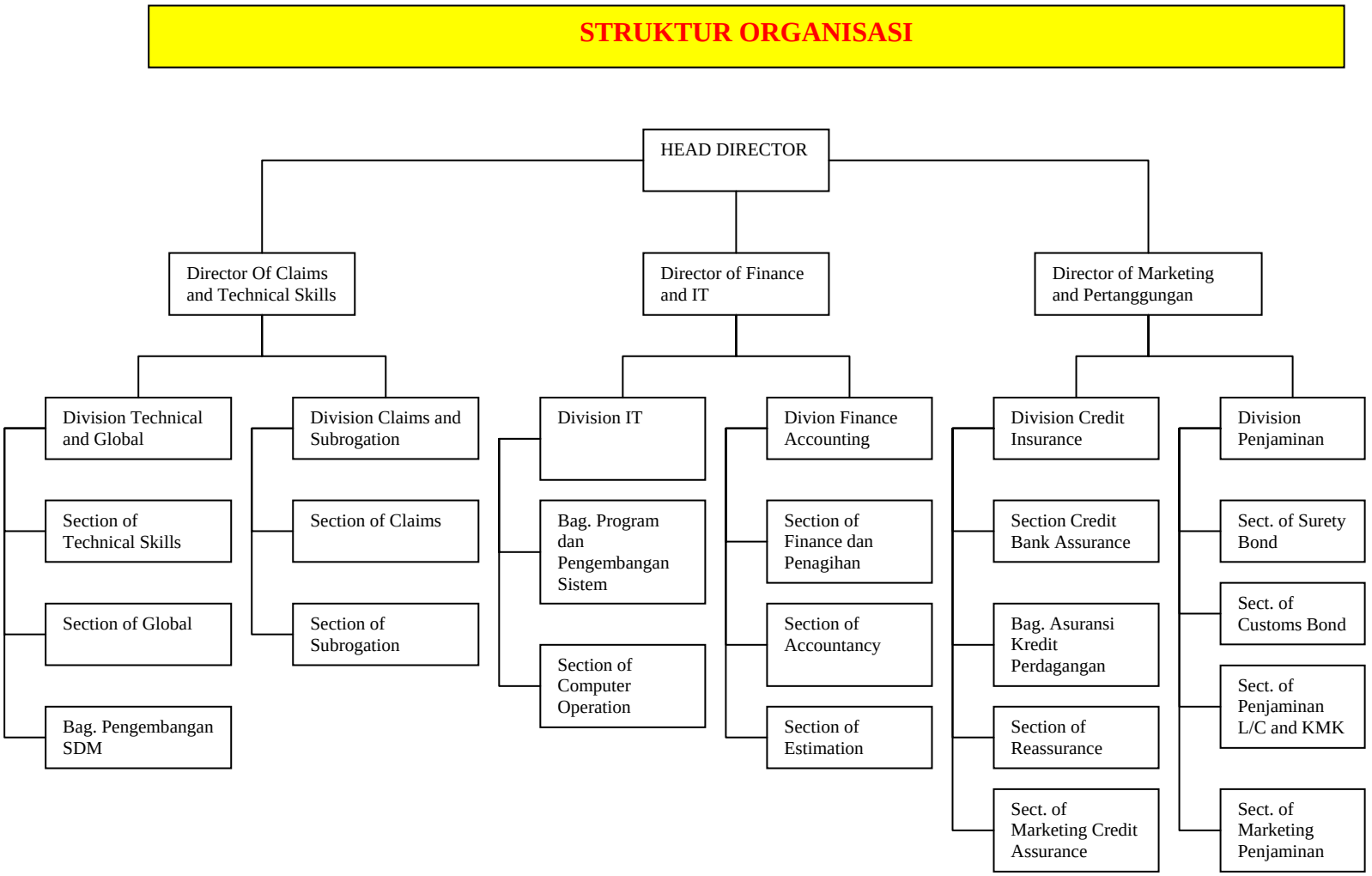
Customs Bond

Memberikanjaminan atas pengguanaan fasilitas kepabeanan, baik oleh importir dan produsen eksportir

Penjaminan L/C Impor & Kredit Modal Kerja (KMK) Ekspor

Menjamin pembayaran L/C Impor dan SKBDN yang telah dibuka oleh Bank dalam megeri, terutama dalam mengimpopr/membeli barang-barang yang digunakan sebagai bahan baku/penolong produksi barang ekspor. Jasa ini Juga menjamin pemberian kredit modal kerja yang digunakan teruatam untuk produksi barang ekspor.

1.4. Struktur Organisasi Perusahaan



1.5. Rincian Personil Perusahaan

NO	KODE	POSISI
1	A01	HEAD DIRECTOR
2	A02	DIRECTOR OF CLAIMS AND TECHNICAL SKILLS
3	A03	DIRECTOR OF FINANCE AND IT
4	A04	DIRECTOR OF MARKETING AND PERTANGGUNGAN
5	A05	KEPALA DIVISI TECHNICAL AND GLOBAL
6	A06	KEPALA DIVISI CLAIMS AND SUBROGATION
7	A07	KEPALA DIVISI IT
8	A08	KEPALA DIVISI FINANCE AND ACOUNTING
9	A09	KEPALA DIVISI CREDIT INSURANCE
10	A10	KEPALA DIVISI PENJAMINAN
11	A11	KEPALA SEKSI TECHNICAL SKILLS
12	A12	KEPALA SEKSI GLOBAL
13	A13	KEPALA SEKSI PENGEMBANGAN SDM
14	A14	KEPALA SEKSI CLAIMS
15	A15	KEPALA SEKSI SUBROGATION
16	A16	KEPALA SEKSI PROGRAM DAN PENGEMBANGAN SISTEM
17	A17	KEPALA SEKSI COMPUTER OPERATION
18	A18	KEPALA SEKSI FINANCE DAN PENAGIHAN
19	A19	KEPALA SEKSI ACCOUNTANCY
20	A20	KEPALA SEKSI ESTIMATION
21	A21	KEPALA SEKSI CREDIT BANK INSURANCE
22	A22	KEPALA SEKSI ASURANSI KREDIT PERDAGANGAN
23	A23	KEPALA SEKSI REASSURANCE
24	A24	KEPALA SEKSI MARKETING CREDIT
25	A25	KEPALA SEKSI SURETY BOND
26	A26	KEPALA SEKSI CUSTOMS BOND
27	A27	KEPALA SEKSI PENJAMINAN L/C DAN KMK
28	A28	KEPALA SEKSI MARKETING PENJAMINAN
29	A29	STAFF SEKSI TECHNICAL SKILLS
30	A30	STAFF SEKSI TECHNICAL SKILLS
31	A31	STAFF SEKSI GLOBAL
32	A32	STAFF SEKSI GLOBAL
33	A33	STAFF SEKSI PENGEMBANGAN SDM
34	A34	STAFF SEKSI PENGEMBANGAN SDM
35	A35	STAFF SEKSI CLAIMS
36	A36	STAFF SEKSI CLAIMS
37	A37	STAFF SEKSI SUBROGATION
38	A38	STAFF SEKSI PROGRAM DAN PENGEMBANGAN SISTEM
39	A39	STAFF SEKSI PROGRAM DAN PENGEMBANGAN SISTEM
40	A40	STAFF SEKSI COMPUTER OPERATION
41	A41	STAFF SEKSI COMPUTER OPERATION
42	A42	STAFF SEKSI FINANCE DAN PENAGIHAN
43	A43	STAFF SEKSI FINANCE DAN PENAGIHAN
44	A44	STAFF SEKSI ACCOUNTANCY
45	A45	STAFF SEKSI ACCOUNTANCY
46	A46	STAFF SEKSI ESTIMATION
47	A47	STAFF SEKSI CREDIT BANK INSURANCE
48	A48	STAFF SEKSI ASURANSI KREDIT PERDAGANGAN
49	A49	STAFF SEKSI REASSURANCE

50	A50	STAFF SEKSI MARKETING CREDIT
51	A51	STAFF SEKSI SURETY BOND
52	A52	STAFF SEKSI CUSTOMS BOND
53	A53	STAFF SEKSI PENJAMINAN L/C DAN KMK
54	A54	STAFF SEKSI MARKETING PENJAMINAN
55	A55	KEAMANAN DIVISI TECHNICAL AND GLOBAL
56	A56	KEAMANAN DIVISI CLAIMS AND SUBROGATION
57	A57	KEAMANAN DIVISI IT
58	A58	KEAMANAN DIVISI FINANCE AND ACOUNTING
59	A59	KEAMANAN DIVISI CREDIT INSURANCE
60	A60	KEAMANAN DIVISI PENJAMINAN

BAB II
PROTEKSI DAN KEAMANAN SISTEM INFORMASI

2.1. Security Management Practices

2.1.1. Overview

Domain *Security Management Practices* menjabarkan tentang proses identifikasi aset perusahaan pada umumnya dan aset informasi perusahaan pada khususnya, serta pengembangan dan implementasi dari kebijakan, standar, panduan dan prosedur untuk menentukan tingkat pengamanannya.

Pada PT. XYZ yang bergerak dalam bidang asuransi, aset informasi merupakan aset yang paling penting dalam perusahaan dan menjadi nilai strategis bagi perusahaan dalam kompetisi dengan perusahaan asuransi sejenis. Oleh karena itu faktor penting dalam nilai suatu informasi (yaitu: kerahasiaan, integritas, dan ketersediaan) merupakan faktor yang harus dikelola dengan baik oleh perusahaan melalui implementasi kebijakan keamanan, agar informasi penting perusahaan terlindung dari berbagai ancaman.

2.1.2. Identifikasi Asset Perusahaan

Aset pada PT. XYZ terdiri atas dua jenis, yaitu:

A. Aset Fisik

1. Ruang kantor. PT. XYZ menempati satu lantai dari suatu gedung yang berlokasi di kawasan bisnis segitiga emas Jakarta dengan luas total ruangan yaitu 500 m2. Ruangan kantor memiliki dua akses lift yaitu lift penumpang dan lift barang, keduanya berhadapan langsung dengan meja jaga satpam, sehingga akses pintu masuk selalu dapat diawasi. Masing-masing divisi pada perusahaan menempati masing-masing satu ruangan besar yang disekat partisi berdasarkan section nya, yaitu ruang divisi Technical and Global, ruang divisi Claims and Subrogation, ruang divisi IT, ruang divisi Finance and Accounting, ruang divisi Credit Insurance, dan ruang divisi penjaminan. Selain itu juga terdapat ruang direktur utama, satu

ruang rapat, satu ruang tamu, dapur, WC, dan gudan kecil untuk menyimpan berbagai perlengkapan kantor, pada bagian depan juga terdapat ruang tunggu tamu yang menyatu dengan ruang resepsionis dan ruang jaga satpam. Server perusahaan, router, modem ADSL terdapat pada ruang server yang berada di dalam ruang divisi IT dan selalu dalam keadaan terkunci.

2. 1 buah server yang disimpan di ruang server perusahaan yang selalu dalam keadaan terkunci.
3. 55 buah PC client desktop berbasis Intel Pentium IV.
4. 4 buah PC Notebook yang masing-masing digunakan oleh direksi.
5. 6 buah printer laser yang masing-masing diletakkan di masing-masing divisi.
6. 2 buah printer *dot matrix* yang diletakkan di divisi Finance and Accounting dan di divisi Credit Insurance.
7. 5 buah printer inkjet yang diletakkan di masing-masing ruangan direksi.
8. 4 buah kamera digital yang digunakan untuk keperluan survey claim asuransi.
9. 2 scanner tipe flatbed yang diletakkan di ruang Divisi Technical and Global dan di ruang divisi IT
10. 1 buah UPS 1200 VA yang digunakan untuk server.
11. 2 modem ADSL yang menyatu dengan 1 port router dan firewall, 1 buah digunakan dalam operasional, 1 buah lagi digunakan sebagai cadangan apabila satu mengalami kerusakan.
12. 1 modem dial up yang digunakan apabila sambungan internet ADSL mengalami gangguan.
13. 2 mesin facsimile yang diletakkan di ruang divisi Claims and Subrogation dan di ruang divisi Credit Insurance.
14. Sambungan telepon 16 line.
15. Sambungan Listrik.
16. Sambungan internet ADSL 512 kbps unlimited.
17. 50 Pesawat telepon.

18. Infrastruktur LAN (Local Area Network).
19. Infrastruktur PABX (Private Automatic Branch Exchange).

B. Aset Informasi
   1. Sistem operasi untuk server yaitu: Redhat Enterprise Linux 4 for Server
   2. Sistem operasi untuk client yaitu: Redhat Enterprise Linux 4 for Desktop
   3. Aplikasi perkantoran : Staroffice.
   4. Aplikasi accounting and finance
   5. Aplikasi asuransi kredit terintegrasi.
   6. Informasi data keuangan dan akunting.
   7. Informasi data asuransi kredit.
   8. Dokumentasi operasional IT
   9. Dokumen sensitif perusahaan seperti surat izin usaha, surat kontrak, surat perjanjian dsb.

2.1.3. Ancaman-ancaman Terhadap Asset Perusahaan

Jenis-jenis ancaman yang dapat terjadi pada PT. XYZ, yaitu:

1. Pencurian

   Pencurian dapat berupa pencurian aset fisik perusahaan dan juga berupa pencurian data perusahaan. Pencurian aset fisik secara langsung mengakibatkan kerugian material bagi perusahaan sedangkan pencurian data perusahaan selain berakibat kerugian material juga berakibat kerugian yang sulit diukur secara material seperti penyalahgunaan nama perusahaan, pencemaran nama baik perusahaan dan jatuhnya informasi penting ke tangan kompetitor.

2. Kehilangan data.

   Kehilangan data penting perusahaan dapat disebabkan oleh beberapa hal seperti kegagalan pada perangkat keras, malfungsi dari aplikasi, kesalahan pengguna sehingga data terhapus secara tidak sengaja, serangan virus dan sebagainya.

3. Pengubahan data yang tidak diinginkan.

   Pengubahan data yang tidak diinginkan dapat terjadi secara sengaja maupun tidak sengaja. Hal ini mengancam integritas dari data yang

dalam prakteknya lebih berakibat fatal daripada hilangnya data, terutama untuk bisnis asuransi yang mengutamakan integritas dan keaslian data.

4. Penggunaan sumber daya komputer yang tidak semestinya.
   Misalnya penggunaan komputer dan akses internet untuk hal-hal di luar kegiatan pekerjaan, penggunaan email perusahaan untuk hal-hal di luar pekerjaan, penggunaan akses level terhadap sistem informasi perusahaan untuk melanggar kerahasiaan informasi perusahaan.
5. Serangan dari luar
   Misalnya port scanning, pengamatan dari luar untuk mendapatkan informasi tentang infrastruktur IT perusahaan, demon dialing untuk mengetahui sambungan modem yang tidak terproteksi, masuknya kode-kode jahat dan virus.

2.1.4. Implementasi Kebijakan Keamanan

Kebijakan keamanan merupakan dasar dari implementasi keamanan yang bersifat teknis, penyusunan kebijakan keamanan ini menjadi begitu penting agar pengaturan keamanan menjadi lebih efektif dan terfokus.

2.1.4.1.Kebijakan (*Policies*)

Kebijakan (Policy) keamanan merupakan tingkat paling atas dan paling pertama dari level dokumentasi yang merupakan visi dan aspek strategis dari keamanan dimana aspek taktis yang lain (prosedur, standar, dan panduan) diturunkan dari sini. Karena mengandung aspek strategis maka dukungan dari manajemen puncak atas kebijakan keamanan ini menjadi begitu penting bagi kelangsungan perusahaan. Manajemen puncak harus menyadari pentingnya implementasi keamanan dan secara terbuka menyatakan dukungannya terhadap implementasi keamanan.

Beberapa kebijakan yang dapat dikembangkan pada PT. XYZ, antara lain:

1. Kebijakan penggunaan komputer

Kebijakan ini secara garis besar mengatur penggunaan komputer pada PT. XYZ, misalnya pihak yang diperkenankan menggunakan komputer, ruang lingkup penggunaan komputer, dan sebagainya.

2. Kebijakan penggunaan sambungan internet dan email.

   Kebijakan ini bertujuan untuk mencegah penggunaan sambungan internet dan email yang tidak semestinya, yang dapat merugikan perusahaan.

3. Kebijakan password

   Kebijakan ini mengatur cara penggunaan password, dan pembuatan strong password, penyimpanan password, frekuensi penggantian password, dan sebagainya.

4. Kebijakan keamanan data

   Kebijakan ini mengatur tentang pengamanan data terhadap ancaman kehilangan dan perubahan yang tidak diinginkan baik yang disengaja maupun yang tidak disengaja.

5. Kebijakan keamanan server dan jaringan.

   Kebijakan ini mengatur tentang pengamanan server dan jaringan berdasarkan akses level yang sudah baku dan sudah diatur berdasarkan peranan pekerjaan/deskripsi pekerjaan.

6. Kebijakan keamanan fisik

   Kebijakan ini mengatur tentang pengamanan aset secara fisik, misalnya penjelasan peran dan tanggung jawab dalam perlindungan aset fisik.

2.1.4.2.Prosedur (*Procedures*)

Prosedur merupakan langkah-langkah detail yang harus diikuti dalam melakukan tugas tertentu. Tujuan dari prosedur adalah memberikan langkah-langkah spesifik untuk menerapkan kebijakan, standar, dan panduan yang sebelumnya sudah dibuat. Pada PT. XYZ prosedur belum dibuat secara baku, sehingga pelaksanaan tugas tertentu dilakukan secara berbeda-beda. Prosedur yang dapat dikembangkan pada PT. XYZ antara lain:

1. Prosedur scanning komputer terhadap virus.

2. Prosedur backup data pada server.
3. Prosedur pemasangan perangkat keras baru.
4. Prosedur instalasi aplikasi.
5. Prosedur menghadapi bencana kebakaran, banjir, huru hara dll.
6. Prosedur pembuatan password.
7. Prosedur penggantian perangkat keras yang rusak.
8. Prosedur penyimpanan file.

2.1.4.3.Standar (*Standards*)

Standar menentukan penggunaan teknologi perangkat keras dan perangkat lunak tertentu secara seragam. Standar biasanya bersifat wajib dan diterapkan secara keseluruhan pada organisasi. Dengan adanya standar maka dapat memudahkan penanganan perangkat keras dan lunak dalam perawatannya karena prosedur untuk penanganannya dapat diseragamkan juga. Pada PT. XYZ standar belum diterapkan secara keseluruhan pada perusahaan. Hal ini disebabkan masih digunakannya beberapa perangkat keras lama dan *legacy system*.

2.1.4.4.Panduan (*Guidelines*)

Panduan hampir mirip dengan standar, tetapi tidak bersifat wajib dan hanya berupa rekomendasi untuk melakukan suatu tindakan. Panduan yang dapat dikembangkan pada PT. XYZ yaitu: panduan untuk mencegah penyebaran virus, panduan penggunaan media penyimpanan portable.

2.2. Access Control Systems and Methodology

2.2.1. Overview

Kontrol akses merupakan mekanisme dan metode untuk mengendalikan akses terhadap sistem informasi perusahaan, sehingga kerahasiaan, integritas, dan ketersediaan informasi dapat dilindungi dari pihak-pihak yang tidak berwenang.

2.2.2. Controls

2.2.2.1.Administrative Control

Pada PT. XYZ administrative control dilakukan dengan:

- Melakukan pemeriksaan latar belakang calon karyawan
- Melakukan pelatihan pemahaman akan pentingnya keamanan
- Penjadwalan cuti
- Rotasi pekerjaan dan pembagian tanggung jawab pekerjaan
- Penandaan dokumen sensitif/rahasia.

2.2.2.2.Technical Control

Pembatasan lima kali kesalahan pada login. Apabila user salah memasukkan username atau password selama lima kali berturut-turut pada kurun waktu 1 jam maka user tersebut akan diblokir tidak dapat masuk ke dalam sistem selama 24 jam berikutnya. Aktivitas ini akan dicatat pada log untuk keperluan audit.

2.2.2.3.Physical Control

- Penggunaan CCTV untuk memantau aktivitas pada tempat yang sensitif keamanannya, misalnya: pada ruang server.
- Penggunaan magnetic ID card untuk dapat memasuki ruang server.

2.2.3. Identifikasi, Otentifikasi, Otorisasi, dan Akuntabilitas

2.2.3.1.Identifikasi

Identifikasi merupakan mekanisme untuk mengenali subyek (pengguna, sistem) sebelum memperoleh akses ke sistem informasi. Identifikasi yang digunakan pada PT. XYZ

adalah *username,* yang dibuat oleh staff seksi computer operation

2.2.3.2.Otentifikasi

Otentikasi merupakan mekanisme verifikasi untuk membuktikan bahwa identitas yang di klaim oleh subyek untuk masuk ke dalam sistem informasi adalah benar. Otentikasi melakukan verifikasi berdasarkan tiga tipe faktor, yaitu:

1. Sesuatu yang diketahui (*Something you know*)
   Misalnya: PIN (*Personal Identification Number*) atau password.
2. Sesuatu yang dimiliki (*Something you have*)
   Misalnya: kartu akses
3. Sesuatu yang menunjukkan ciri seseorang secara fisik
   Misalnya: sidik jari atau retina scan

Pada PT. XYZ proses otentikasi dilakukan dengan melibatkan satu faktor verifikasi yaitu dengan menggunakan password. Pembuatan password oleh masing-masing pengguna harus mengikuti kebijakan dan prosedur pembuatan password yang telah ditentukan sebelumnya.

2.2.3.3.Otorisasi

Otorisasi merupakan proses pemberian hak kepada subyek untuk melakukan akses terhadap sistem informasi sesuai dengan level akses yang telah ditentukan sebelumnya. Proses otorisasi dilakukan dengan mengacu pada *access control matrix* yang merupakan suatu tabel yang menerangkan tindakan yang dapat dilakukan oleh subyek terhadap sistem informasi. Pada PT. XYZ access control matrix dijabarkan sebagai berikut:

Divisi	**Level**	A	B	C	D	E	F
	Direksi	Full	Full	Full	Full	Full	Full
Technical and Global	Kepala Divisi	NA	Full	NA	Full	NA	NA
	Kepala Seksi	NA	RWA	NA	RWA	NA	NA
	Staff Seksi	NA	RWA	NA	RWA	NA	NA
Claims and Subrogation	Kepala Divisi	R	Full	R	Full	NA	NA
	Kepala Seksi	R	RWA	R	RWA	NA	NA
	Staff Seksi	NA	RWA	NA	RWA	NA	NA
IT	Kepala Divisi	Full	Full	NA	NA	Full	NA
	Kepala Seksi	Full	Full	NA	NA	Full	NA
	Staff Seksi	Full	Full	NA	NA	Full	NA
Finance Accounting	Kepala Divisi	Full	Full	Full	Full	NA	NA
Divisi	**Level**	A	B	C	D	E	F
	Kepala Seksi	RWA	RWA	RWA	RWA	NA	NA
	Staff Seksi	RWA	RWA	RWA	RWA	NA	NA
Credit Insurance	Kepala Divisi	R	Full	R	Full	NA	NA
	Kepala Seksi	R	RWA	R	RWA	NA	NA
	Staff Seksi	NA	RWA	NA	RWA	NA	NA
Penjaminan	Kepala Divisi	R	Full	R	Full	NA	NA
	Kepala Seksi	R	RWA	R	RWA	NA	NA
	Staff Seksi	NA	RWA	NA	RWA	NA	NA

Keterangan:

A = Aplikasi accounting and finance

B = Aplikasi asuransi kredit terintegrasi.

C = Data keuangan dan akunting.

D = Data asuransi kredit.

E = Dokumentasi operasional IT

F = Dokumen sensitive perusahaan seperti surat izin usaha, surat kontrak, surat perjanjian dsb.

R = Read

W = Write

A = Alter

D = Delete

NA = No Access

Full = Read, Write, Alter, Delete

2.2.3.4.Akuntabilitas

Akuntabilitas merupakan mekanisme untuk mencatat setiap aktivitas yang dilakukan oleh pengguna. Pencatatan ini dapat mempermudah proses audit terhadap system informasi dimana semua aktivitas dari setiap pengguna dapat dipertanggungjawabkan.

2.3. Telecomunications and Network Security

2.3.1. Overview

Domain ini menjabarkan aspek keamanan dalam infrastruktur jaringan dan telekomunikasi untuk menjamin kerahasiaan, integritas dan ketersediaan data.

2.3.2. Peralatan Jaringan dan Telekomunikasi

Peralatan jaringan dan telekomunikasi yang digunakan pada PT. XYZ adalah sebagai berikut :

1. 10 buah server dari berbagai tipe dengan fungsi masing-masing diantaranya adalah yang berbasis Intel Xeon Dual Processor 3.0 Ghz, 4x36 GB SCSI HDD, 1 GB RAM
2. 30 buah PC notebook
3. 224 buah PC client desktop berbasis Intel Pentium IV
4. 30 buah printer laser yang masing-masing diletakkan di masing-masing divisi.
5. 81 buah printer dot matrix yang tersebar di divisi Finance and Accounting dan di divisi Credit Insurance dan divisi lainnya
6. 30 buah printer inkjet yang diletakkan di masing-masing ruangan direksi, masing-masing kepala biro, dan kepala seksi.
7. 10 buah UPS 1200 VA yang digunakan untuk server.

8. 2 modem ADSL yang menyatu dengan 1 port router dan firewall, 1 buah digunakan dalam operasional, 1 buah lagi digunakan sebagai cadangan apabila satu mengalami kerusakan.
9. 10 modem dial up yang digunakan apabila sambungan internet ADSL mengalami gangguan.
10. 2 mesin facsimile yang diletakkan di ruang divisi Claims and Subrogation dan di ruang divisi Credit Insurance.
11. Sambungan telepon 16 line.
12. Sambungan Listrik.
13. Sambungan internet ADSL 512 kbps unlimited.
14. 225 Pesawat telepon.
15. Infrastruktur LAN (Local Area Network).
16. Infrastruktur PABX (Private Automatic Branch Exchange).

2.3.3. Keamanan Jaringan

Untuk meningkatkan keamanan jaringan pada PT. XYZ maka dapat dilakukan hal-hal sebagai berikut:

- Menambahkan Intrusion Detection System (IDS) berbasis jaringan untuk mendeteksi adanya intrusi dari luar jaringan perusahaan.
- Melakukan update antivirus dan operating system secara teratur pada setiap host.
- Melakukan update patch database secara teratur.
- Menambahkan Personal Firewall yang berupa software pada masing-masing host.
- Penggunaan Teknologi RAID pada media penyimpanan pada server, direkomendasikan menggunakan teknologi RAID 10 (*Striping Across Multiple Pairs* / 1+0) untuk memperoleh performansi dan redundansi data sekaligus.
- Meningkatkan pengamanan secara fisik pada ruangan server dengan memasang kamera CCTV dan penggunaan magnetic card ID untuk membatasi akses masuk ke ruang server.

- Menggunakan proxy server untuk mengatur dan memfilter akses internet.
- Menerapkan aturan-aturan pada Firewall yang ketat, yaitu dengan memeriksa konfigurasi firewall secara berkala dan selalu memblok port-port akses ke database.

2.4. Cryptography

Domain ini membahas aspek keamanan sistem informasi dari sisi penyandian dan penyembunyian data dengan menggunakan teknik cryptography. Tujuan dari cryptography ini adalah agar informasi yang disampaikan hanya dapat dibaca dan dimengerti oleh pihak yang dituju.

Pada PT. XYZ, penerapan cryptography dilakukan pada proses pengiriman email dengan menggunakan *digital signature*, selain itu enkripsi data juga dilakukan pada website dari PT. XYZ pada saat transmisi data dari web server ke web browser klien dengan menggunakan teknologi SSL (*Secure Socket Layer*) sehingga apabila data penting klien PT. XYZ disadap pada saat transmisi, penyadapnya tidak dapat membaca isi dari data tersebut. Pada sistem aplikasi pada PT. XYZ juga telah menerapkan enkripsi data, tetapi enkripsi data pada database aplikasi tersebut masih terbatas pada enkripsi password saja yang sudah dikembangkan pada saat pengembangan aplikasi.

2.5. Security Architecture and Models

Tujuan dari domain ini adalah untuk mempelajari konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi dan sistem yang aman. Penerapan *security architecture* dan model yang baik akan sangat membantu keamanan sistem perusahaan secara keseluruhan.

Keamanan yang diterapkan sesuai *security architecture and model* ini yaitu:

- Pada sisi SDMnya yaitu para pegawai yang bekerja di perusahaan ini dibekali dengan standar-standar tentang keamanan. Jadi tiap karyawan diharapkan dapat sadar akan pentingnya keamanan. Misalnya tidak meninggalkan komputer/sistem dalam keadaan login. Tidak menuliskan password. Tidak

menggunakan password yang mudah ditebak. Mengganti password secara teratur, misal sebulan sekali. Tidak membicarakan tentang sistem keamanan di perusahaan ke orang lain yang tidak berhak. Dan lain-lain.

- Proteksi pada komputer/sistem dilakukan agar hanya karyawan yang berwenang yang dapat mengakses komputer/sistem tersebut. Karyawan tersebut diberikan username dan password untuk mengakses.
- Penggunaan firewall antara jaringan lokal ke internet untuk menambah keamanan pada jaringan lokal
- Penggunaan personal firewall dan anti virus pada komputer pribadi untuk mencegah tertular virus dan untuk memantau/membatasi hak akses ke komputer tersebut melalui jaringan.

2.6. Operation Security

Operation security adalah kegiatan sehari-hari yang dilakukan agar sistem dapat berjalan dengan aman, setelah infrastruktur TI diimplementasikan.
Operation security yang diterapkan di perusahaan ini antara lain:

- Penggunaan ID card untuk setiap karyawan.
- Absensi datang dan pulang.
- Auto update patch untuk sistem operasi yang digunakan.
- Auto update anti virus database.
- Mencatat/mendokumentasikan setiap perubahan yang terjadi.
- Melakukan backup harian/mingguan untuk server-server yang ada sebanyak 2 kopi untuk disimpan oleh 2 karyawan yang berbeda.

2.7. Application and System Development Security

Perusahaan asuransi ini mengembangkan sendiri aplikasi yang digunakan untuk sistem perasuransiannya. Aplikasi ini di install ke sebuah server utama yang digunakan oleh perusahaan ini. Dalam menginstall server juga diperhatikan masalah keamanan. Misalnya update terbaru untuk sistem operasi yang digunakan. Menutup semua port yang tidak digunakan oleh aplikasi tersebut agar mengurangi back door yang dapat digunakan oleh hacker. Pemberian password server yang tidak mudah ditebak dengan panjang minimum 10 karakter. Pengupdatean Keamanan untuk hal ini dilakukan dengan mengupdate aplikasi dengan patch terbaru, penggunaan login.
Berikut adalah tabel portfolio aplikasi yang dipakai oleh perusahaan ini:

ENTERPRISE MANAGEMENT
Corporate Portal Workgroup Collaboration Document Management Knowledge Management Business Forecasting / Simulation Help Desk CRM

APLIKASI OPERASIONAL
Asuransi Kredit Asuransi Kredit Perdagangan Reasuransi Surety Bond Custom Bond & LC Klaim & Subrogasi

SUPPORT		
KEUANGAN	SDM	UMUM
General Ledger Account Receivable Account Payable Asset Management	Payroll Re-Design Personnel Employee Benefit Career Path	Inventory Procurement

PERENCANAAN	KONTROL
E.D.I Biro P.P	Audit OLAP (OP) OLAP (Support)

2.8. Disaster Recovery and Business Continuity Plan

Domain ini membahas bagaimana dan apa yang dilakukan untuk meminimalisasi bencana atau apabila terjadi bencana.

- Tape backup tidak disimpan di kantor, tetapi dibawa oleh 2 orang karyawan yang berbeda.
- Mencatat nomor telepon setiap karyawan yang ada dan ditempelkan di suatu tempat yang mudah dilihat.

- Pemakaian genset dan UPS jika terjadi permasalahan dengan listrik PLN.
- Disediakannya alat pemadam api di tempat-tempat yang strategis dan menempelkan nomor telepon pemadam kebakaran dan kepolisian di dekat alat pemadam kebakaran tersebut.
- Pelatihan karyawan apabila terjadi bencana kebakaran. Tentang apa yang harus diselamatkan dan bagaimana cara menyelamatkan diri.

2.9. Laws, Investigations, and Ethics

Pada domain ini dibahas mengenai berbagai jenis masalah ataupun aturan yang berhubungan dengan kejahatan komputer, perlindungan hak cipta dan legalitas transaksi elektronik.

Kemungkinan-kemungkinan adanya hal-hal yang berkaitan dengan masalah-masalah tersebut diatas yang dapat terjadi di perusahaan asuransi PT. XYZ adalah sebagai berikut:

- Pencurian data, secara softcopy maupun hardcopy yang dapat terjadi melalui berbagai sarana. Seperti misalnya pihak luar yang menyusup masuk kedalam jaringan konputer internal perusahaan. Ataupun pencurian data secara fisik seperti hasil print out dari database pelanggan
- Pengubahan data pada database perusahaan
- Menulari sistem komputer perusahaan dengan virus, memasukkan worm, trojan atau hal-hal yang berkaitan dengan yang seperti ini.
- Perusakan sistem secara fisik.

Usaha-usaha yang bersifat antisipatif terhadap hal-hal seperti disebut diatas dilakukan dengan penerapan kebijakan-kebijakan yang berkaitan dengan penggunakan komputer, jaringan, aplikasi, dan lain sebagainya.

Perusahaan juga mematuhi undang-undang mengenai hak cipta dengan menghindari pemakaian perangkat lunak bajakan.

2.10. Physical Security

Physical security berkaitan erat dengan sarana dan prasarana sistem informasi. Hal-hal yang berkaitan dengan penempatan server-server aplikasi maupun database, usaha-usaha apa saja yang dilakukan untuk mencegah terjadinya akses data ataupun sistem oleh pihak-pihak yang tidak berhak, dan sebagainya.

Berikut adalah daftar dari berbagai jenis server yang digunakan oleh perusahaan:

NO	SERVER NAME	FUNCTION	STORAGE SIZE
1	XYZ1	Database Investasi	2 x 10 GB
2	XYZ2	Database Penjaminan	4 x 18 GB
3	XYZ2	Database PUKK, SDM, OK, Akuntansi, Askredag	4 x 18 GB
4	CITRIX1	Citrix	6 x 18 GB
5	XYZ3	Database SIM	6 x 18 GB
6	XYZ4	Database Koperasi, Askred	6 x 18 GB
7	XYZ5	E A Server	6 x 36 GB
8	XYZ6	Database Integrasi Data	6 x 36 GB
9	XYZJKT	Internet Server	1 x 4 GB
10	MDAEMON	Mail Server	3 x 9 GB

Prosedur pemakaian sistem dan semua hal yang berkaitan dengan sistem informasi harus dibuat dengan rinci dan harus benar-benar diterapkan pada perusahaan.

Pengamanan sistem dilakukan secara fisik, yaitu dengan:

1. Menempatkan server-server pada ruang-ruang khusus yang sangat dibatasi aksesnya.
2. Menempatkan penjaga-penjaga keamanan (satpam) pada titik-titik yang merupakan gateway atau pintu masuk untuk daerah-daerah yang dianggap rawan dan penting.
3. Memasang sistem alarm atau tanda bahaya yang dapat mendeteksi adanya penyusup yang berusaha memasuki daerah atau areal-areal yang penting.

Berikut adalah daftar personal computer dan printer yang ada pada perusahaan yang tersebar di semua divisi:

NO	SECTION (DIVISI/BIRO)	TOTAL PC	TOTAL PRINTER
1	BPKP	3	2
2	Claims & Subrogation	36	27
3	Functionary Mount Kadiv	1	0
4	Biro PP	9	3
5	Credit Assurance	28	14
6	Surety	25	18
7	Monitoring Intern	9	4
8	Finance & Accounting	38	23
9	Global & Technical Skill	26	19
10	Secretaries of Company	25	21
11	Information Technology	24	10
	TOTAL	**224**	**141**

2.11. Auditing and Assurance

Audit terhadap proses bisnis yang berkaitan dengan sistem informasi perusahaan sedikitnya lima tahun sekali.

Khususnya pada proses-proses bisnis yang berkaitan dengan finansial dan proses-proses bisnis yang berkaitan erat dengan core bisnis perusahaan. Pelaksanaan audit juga dilakukan dengan mengikuti standar-standar proses audit sistem informasi yang sudah menjadi standar de facto dan dianut secara luas.

Audit pada sistem informasi juga berkaitan erat dengan assurance atau penjaminan bahwa sistem dapat melakukan fungsinya sesuai dengan yang diharapkan.

Hasil-hasil atau temuan-temuan dari proses audit sedapat mungkin ditanggapi dan dilakukan langkah-langkah yang diperlukan agar perusahaan dapat memperoleh manfaat yang sebesar-besarnya dari sistem informasi maupun teknologi informasi yang diterapkan pada perusahaan.