LAMPIRAN

Form Observasi dan Wawancara

Materi Observasi dan wawancara :

1. Profil Perusahaan
2. Pengelolaan Kebijakan Keamanan Informasi
3. Pengelolaan Aset Perusahaan
4. Pengelolaan Sumber Daya Manusia TI
5. Pengelolaan Fisik dan Lingkungan
6. Pengelolaan Komunikasi dan Operasional
7. Pengelolaan Pembangunan Sistem dan Pemeliharaan
8. Pengelolaan Insiden Keamanan Informasi
9. Pengelolaan Keberlansungan Bisnis
10. Identifikasi Ancaman
11. Identifikasi Kelemahan
12. Pemeriksaan Kebutuhan Keamanan
13. Pemeriksaan Kombinasi Kontrol Keamanan
14. Penilaian Kecenderungan dan Dampak
15. Penilaian Risiko

Daftar pertanyaan

1. Profil Perusahaan
   - 1.1 Bagaimana Sejarah singkat perusahaan ?
   - 1.2 Apa visi misi perusahaan ?
   - 1.3 Bagaimana struktur organisasi perusahaan ?
   - 1.4 Apa bisnis inti perusaaan ?

2. Pengelolaan Kebijakan Keamanan Informasi
   - 2.1 Kebijakan apa saja yang telah dijalankan di perusahaan ?

3. Pengelolaan Aset Perusahaan
   - 3.1 Berapa dan apa spesifikasi aset perangkat teknologi informasi (hardware) milik perusahaan ?
   - 3.2 Sistem operasi apa yang digunakan di perusahaan ?
   - 3.3 Apa aplikasi pendukung perkantoran yang digunakan perusahaan ?
   - 3.4 Apa aplikasi pendukung bisnis yang digunakan perusahaan ?
   - 3.5 Bagaimana topologi jaringan komputer yang digunakan perusahaan ?
   - 3.6 Siapa penyelenggara jasa internet yang digunakan perusahaan ?
   - 3.7 Perangkat jaringan apa saja yang digunakan ?
   - 3.8 Fasilitas internet apa saja yang digunakan oleh perusahaan ?
   - 3.9 Protokol internat apa yang digunakan perusahaan ?
   - 3.10 Jenis firewall apa yang digunakan ?
   - 3.11 Bagaimana identifikasi informasi sensitif dan kritikal di perusaahan ?
   - 3.12 Bagaimana komposisi pekerja berdasarkan jabatan
   - 3.13 Bagaimana komposisi pekerja berdasarkan pendidikan
   - 3.14 Sarana pendukung apa yang dimiliki perusahaan ?

4. Pengelolaan Sumber Daya Manusia TI
   - 4.1 Berapa jumlah pengguna aplikasi bisnis di perusahaan ?

5. Pengelolaan Fisik dan Lingkungan
   - 5.1 Bagaimana pembagian ruang TI ?
   - 5.2 Bagaimana lingkungan server/data center ?

6. Pengelolaan Komunikasi dan Operasional
   - 6.1 Apakah terdapat sosilisasi atau pelatihan tentang kebijakan yang terkait dengan keamanan informasi ?

7. Pengelolaan Pembangunan Sistem dan Pemeliharaan
    7.1 Apakah aplikasi bisnis yang digunakan telah memenuhi keamanan informasi?
    7.2 Apakah perusahaan melakukan pengujian keamanan informasi pada aplikasi dan sistem yang digunakan ?
    7.3 Apakah dilakukan pemeliharaan dan evaluasi terhadap gangguan dan kelemahan yang dimiliki aplikasi dan sistem?

8. Pengelolaan Insiden Keamanan Informasi
    8.1 Apakah dilakukan pencatatan dan tindak lanjut pada kejadian gangguan keamanan yang pernah terjadi ?

9. Pengelolaan Keberlansungan Bisnis
    9.1 Apakah perusahaan memiliki rencana penanggulangan terhadap bencana yang mungkin saja terjadi, sehingga terdapat jaminan keberlansungan bisnis dapat tetap berjalan, meski terjadi bencana ?

10. Identifikasi Ancaman

11. Identifikasi Kelemahan

12. Pemeriksaan Kebutuhan Keamanan

13. Pemeriksaan Kombinasi Kontrol Keamanan

14. Penilaian Kecenderungan dan Dampak

15. Penilaian Risiko

Hasil Observasi dan Wawancara

Document Number. v5.0
Create by AanAlBone

Nara sumber: 1. Suwondo W. (Manager Sistem Informasi & Pengadaan)
2. Dahlan (Supervisor Teknologi Informasi)

Waktu : Observasi dan wawancara dilakukan dengan 7 kali pertemuan, selama 3 bulan (Februari sampai April)

1. Profil Perusahaan

1.1 Bagaimana Sejarah singkat perusahaan ?

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

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

1.2 Apa visi misi perusahaan ?

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

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

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

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

1.3 Bagaimana struktur organisasi perusahaan ?

Struktur Organisasi PT Multi Terminal Indonesia

1.4 Apa bisnis inti perusaaan ?

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

2. Pengelolaan Kebijakan Keamanan Informasi

2.1 Kebijakan apa saja yang telah dijalankan di perusahaan ?

Kebijakan Keamanan Informasi Perusahaan

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

3. Pengelolaan Aset Perusahaan

3.1 Berapa dan apa spesifikasi aset perangkat teknologi informasi (hardware) milik perusahaan ?

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

Spesifikasi Server

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

Spesifikasi PC

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

3.2 Sistem operasi apa yang digunakan di perusahaan ?

Sistem Operasi yang digunakan

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

3.3 Apa aplikasi pendukung perkantoran yang digunakan perusahaan ?

Perangkat lunak perkantoran yang digunakan

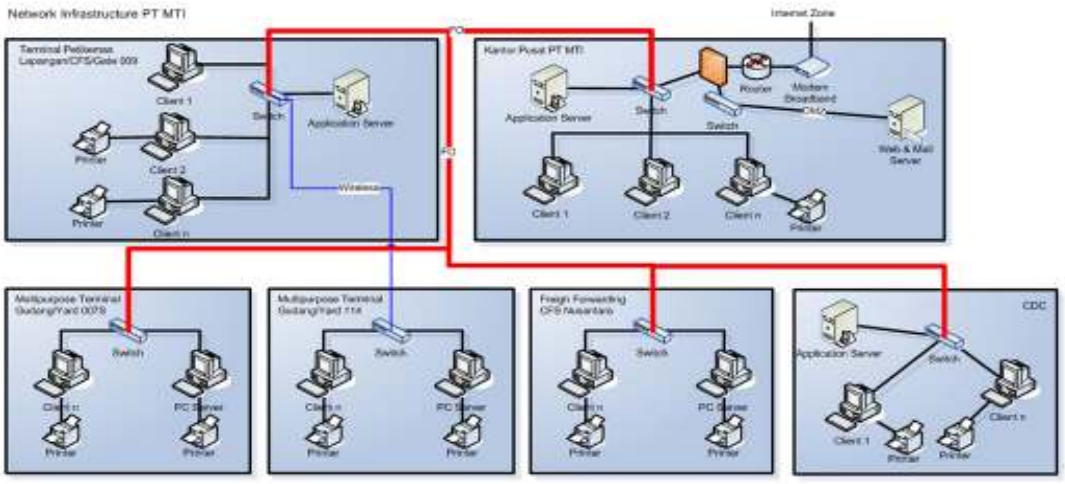
No	Aplikasi Pendukung Perkantoran
1	Microsoft office 97
2	Microsoft Office 2003, XP
3	Microsoft XP
4	Email Server multiterminal.co.id

3.4 Apa aplikasi pendukung bisnis yang digunakan perusahaan ?

Perangkat lunak pendukung bisnis yang digunakan

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

3.5 Bagaimana topologi jaringan komputer yang digunakan perusahaan ?



Topologi Jaringan Komputer Perusahaan

3.6 Siapa penyelenggara jasa internet yang digunakan perusahaan ?

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

3.7 Perangkat jaringan apa saja yang digunakan ?

Perangkat Jaringan Komputer

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

3.8 Fasilitas internet apa saja yang digunakan oleh perusahaan ?

Fasilitas Internet yang digunakan

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

3.9 Protokol internat apa yang digunakan perusahaan ?

Penggunaan Protokol Internet

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

3.10 Jenis firewall apa yang digunakan ?

Firewall yang digunakan

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

3.11 Bagaimana identifikasi informasi sensitif dan kritikal di perusaahan ?

Identifikasi Informasi yang Sensitif dan Kritikal

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

3.12 Bagaimana komposisi pekerja berdasarkan jabatan

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

3.13 Bagaimana komposisi pekerja berdasarkan pendidikan

Komposisi Pekerja Berdasarkan Pendidikan

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

3.14 Sarana pendukung apa yang dimiliki perusahaan ?

Sarana Pendukung

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

4. Pengelolaan Sumber Daya Manusia TI

4.1 Berapa jumlah pengguna aplikasi bisnis di perusahaan ?

Pengguna Sistem Aplikasi pendukung bisnis

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

5. Pengelolaan Fisik dan Lingkungan

5.1 Bagaimana pembagian ruang TI ?

Pembagian Ruang TI

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

5.2 Bagaimana lingkungan server/data center ?

Lingkungan Lokasi Server/Data Center

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

6. Pengelolaan Komunikasi dan Operasional

6.1 Apakah terdapat sosilisasi atau pelatihan tentang kebijakan yang terkait dengan keamanan informasi ?

Sosialisasi keamanan informasi pernah dilakukan, tetapi tidak secara rutin, sehingga pergantian karyawan baru menyebabkan karyawan yang bekerja tidak mengetahui kebijakan atau prosedur keamanan informasi yang diterapkan oleh perusahaan.

7. Pengelolaan Pembangunan Sistem dan Pemeliharaan

7.1 Apakah aplikasi bisnis yang digunakan telah memenuhi keamanan informasi?

Fungsi keamanan informasi pada aplikasi yang dibangun, telah memiliki aspek keamanan, yaitu authentication dan authorization kepada penggunanya, tetapi belum menerapkan ekripsi pada data/informasi rahasia.

7.2 Apakah perusahaan melakukan pengujian keamanan informasi pada aplikasi dan sistem yang digunakan ?

Kontrol Fisik yang digunakan

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

7.3 Apakah dilakukan pemeliharaan dan evaluasi terhadap gangguan dan kelemahan yang dimiliki aplikasi dan sistem?

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

8. Pengelolaan Insiden Keamanan Informasi

8.1 Apakah dilakukan pencatatan dan tindak lanjut pada kejadian gangguan keamanan yang pernah terjadi ?

Bahwa idak dilakukan pencatatan secara sistematis terhadap kejadian terkait dengan keamanan informasi, sehingga kejadian hanya dianalisis dan ditindak secara adhoc.

9. Pengelolaan Keberlansungan Bisnis

9.1 Apakah perusahaan memiliki rencana penanggulangan terhadap bencana yang mungkin saja terjadi, sehingga terdapat jaminan keberlansungan bisnis dapat tetap berjalan, meski terjadi bencana ?

Bahwa perusahaan tidak memiliki rencana penanggulangan bencana, agar bisnis dapat berjalan, meski terjadi bencana, yaitu dengan penyusunan BCP (*Business Continuity Plan)* dan DRP *(Data Recovery Plan)*. Sedangkan untuk *Disaster Recovery Center* (DRC) telah dimiliki saat ini, masih berada pada lokasi yang sama dengan data center, sehingga kerentanan keamanan informasi sangat tinggi.

10. Identifikasi Ancaman

Ancaman Aktif

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

Ancaman Aktif (2)

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

Ancaman Pasif

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

11. Identifikasi Kelemahan

Kelemahan (1)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
1	Industrial espionage/Pengintai	Informasi	Informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka.	Informasi yang akan keluar dari perusahaan, harus terklasifikasi dan dilabelkan berdasarkan sensitifitas, jika tidak, maka informasi tersebut menjadi tidak diproteksi secara baik, menyebabkan hilangnya kerahasiaan informasi.
2	Kegagalan perangkat	Informasi	Tidak memiliki rencana dalam penanggulangan bencana, sehingga tidak ada jaminan bahwa bisnis dapat berjalan secara cepat, setelah terjadi bencana.	Jika terjadi bencana, tidak memilk alternatif cara agar bisnis dapat terus berjalan, sehingga yang terjadi bisnis terhenti dan perusahaan mengalami kerugian.
3	Alam/Bencana Alam: Petir	Fisik: Server	Petir di lokasi tersebut, intensitasnya cukup besar, dan peralatan penangkal (antipetir dan grounding) belum mampu meredamnya.	Server terancam rusak dan terbakar, disebabkan terkena petir.
4	Kegagalan perangkat	Informasi	Perangkat DRC yang masih berada pada ruang yang sama dengan data center dan server	Jika terjadi bencana pada ruang server dan data center, maka DRC dan file backup mengalami bencana yang sama sehingga tidak mampu mengembalikan informasi dan sistem beroperasi kembali.
5	Virus	Software	Sistem operasi yang rentan dengan gangguan virus dan meningkatnya penyebaran virus melalui email, tanpa didukung oleh perangkat antivirus yang cukup handal, dapat menimbulkan kerusakan file, dan kehilangan file data.	Sistem operasi yang rentan dengan penyebaran virus, dapat berpotensi merusak informasi dan mengganggu jaringan komputer perusahaa.
6	Hacker, cracker, insiders	Network & Informasi	Penggunaan firewall hanya pada sisi luar DMZ saja, berpotensi terbukanya wilayah server dari gangguan yang berasal dari dalam jaringan (lokal), karena area dalam DMZ tidak dilindungi firewall	Penyusupan dan gangguan yang berasal dari jaringan lokal dapat langsung masuk ke area DMZ dimana server berada, dan mengakses informasi dan sistem yang sensitif dan kritikal.

Kelemahan (2)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
7	Kegagalan perangkat: Perangkat Lunak	Software: System Backup	Tidak dilakukan pengujian terhadap file hasil backup sistem dan data.	Jika terjadi kehilangan data pada sistem utama, maka hasil backup tidak dapat direstore, terjadi kehilangan informasi.
8	Employee	Hardware & Software & Informasi	Pegawai yang telah menguasai bisnis proses dan pengelolaan teknologinya, masih berstatus pegawai kontrak,	Berpotensi pegawai IT dapat keluar kapan pun dari perusahaan dan divisi IT kekurangan pegawai terlatih.
9	Employee	Software & Karyawan	Karyawan di divisi TI yang cenderung bergant-ganti, sehingga dengan teknologi yang dgunakan oleh perusahaan, membutuhkan keterampilan dan pengetahuan yang cukup, agar dapat melakukan monitoring dan pemeliharaan terhadap sistem yang ada.	Karyawan pengganti atau baru tidak mampu menguasai teknologi perusahaan secara cepat, sehingga proses monitoring dan pemeliharaaan sistem menjadi lambat dan terhambat.
10	Employee	Software & Karyawan	Terjadi kesalahan input data pada aplikasi di lapangan, dan tidak terdapat prosedur tetap dalam pelaporan dan verifikasi kesalahan tersebut.	Kesalahan input data tersebut jika tidak diverifikasi dan dikoreksi secara cepat, menyebabkan waktu layanan menjadi lama, dan akan menurunkan kepercayaan konsumen terhadap perusahaan.
11	Hacker, cracker, Employee	Software & Informasi	Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi,	Perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, menyebabkan kelemahan tersebut diketahui orang, yang akan mengganggu keamanan informasi.
12	Insiders	Informasi	Jika perusahaan memiliki karyawan baru tidak akan pernah mengetahui tentang kebijakan tentang keamanan informasi, karena aturan yang tidak tertulis dan tidak disosialisasikan dengan baik.	Kecerobohan dan kesalahan yang dilakukan karyawan, sehingga menyebabkan gangguan keamanan informasi.

Kelemahan (3)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
13	Vendor	Informasi	Aplikasi yang dibangun dengan platform DBMS yang berbeda dan tidak memenuhi standard keamanan informasi pada aplikasi.	Integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi antar data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai.
14	Insiders	Informasi	Modifikasi informasi dan pencurian informasi melalui komputer yang tidak mengaktifkan keamanan dekstop, saat pemiliknya tidak berada ditempat.	Terjadinya pengamblan, modifikasi dan kehilangan informasi file yang sensitif dan kritikal pada PC tersebut.
15	Kegagalan Perangkat	Hardware & Software & Informasi	Tidak dilakukan pemeliharaan terhadap perangkat pendukung yang kritikal secara rutin dan berkala, seperti pendingin ruangan pada ruang server dan listrik dengan gensetnya.	Pemeliharaan yang tidak dilakukan secara rutin dan berkala terhadap perangkat pendukung, seperti pendingin ruangan, dapat menyebabkan kerusakan secara mendadak, sehingga akan mengganggu terutama ruang yang kritikal seperti data center dan ruang server.
16	Insiders	Informasi	Informasi yang sensitif (rahasia) dapat dilakses dan dicuri oleh orang yang tidak berhak, karena informasi dilindungi oleh teknologi enkripsi pada informasi tersebut.	Informasi sensitif yang dibaca oleh orang yang tidak berhak, akan menyebabkan menurunnya kepercayaan konsumen terhadap perusahaan.

Kelemahan (4)

No	Sumber Ancaman	Aset	Kelemahan/Kerawanan (Vulnerability)	Ancaman (Threat)
17	Hacker, cracker, insiders	Network & Informasi	Tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.	Tidak diaktifkannya PC firewall, dapat memudahkan masuknya akses yang tidak terotorisasi, sehingga dapat menyebabkan hilangnya informasi, atau modifikasi dan kerusahakan sistem dan informasi.
18	Kegagalan perangkat	Hardware & Software	Penggunaan aplikasi dan transaksi informasi yang terus bertambah, tidak terukur secara baik, sehingga sulit mengetahui kinerja dan beban sistem saat ini.	Kinerja sistem aplikasi dan transaksi data dapat menurun dan mati tiba-tiba, karena tidak pernah terukur secara baik penambahan beban dari waktu ke waktu.
19	Insiders	Karyawan & software	Operator yang berstatus kontrak, berjumlah cukup banyak, dengan penugasan harian, cenderung rentan dengan penyalahgunaan.	Setiap operator diberikan otentikasi dan otorisasi dalam menggunakan aplikasi dan infirmasi, jika tidak diawasi secara baik, dapat berpotensi menjadi insiders yang mengganggu keamanan informasi.

12. Pemeriksaan Kebutuhan Keamanan

Hasil Permeriksaan Kriteria Keamanan Informasi (1)

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

Hasil Pemeriksanaan Kriteria Keamanan Informasi (2)

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

13. Pemeriksaan Kombinasi Kontrol Keamanan

Tabel Kombinasi Kontrol (1)

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

Tabel Kombinasi Kontrol (2)

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

14. Penilaian Kecenderungan dan Dampak

Tingkatan Likelihood

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

Ukuran dari Dampak

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

Kecenderungan dan Dampak (1)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
1	Informasi yang berada didalam perusahaan, tidak terklasifikasi dengan baik berdasarkan aspek kerahasiaannya, maka dapat berpotensi informasi rahasia dapat terbuka.	Informasi yang akan keluar dari perusahaan, harus terklasifikasi dan dilabelkan berdasarkan sensitifitas, jika tidak, maka informasi tersebut menjadi tidak diproteksi secara baik, menyebabkan hilangnya kerahasiaan informasi.	4	4	16
2	Tidak memiliki rencana dalam penanggulangan bencana, sehingga tidak ada jaminan bahwa bisnis dapat berjalan secara cepat, setelah terjadi bencana.	Jika terjadi bencana, tidak memilk alternatif cara agar bisnis dapat terus berjalan, sehingga yang terjadi bisnis terhenti dan perusahaan mengalami kerugian.	4	4	16
3	Petir di lokasi tersebut, intensitasnya cukup besar, dan peralatan penangkal (antipetir dan grounding) belum mampu meredamnya.	Server terancam rusak dan terbakar, disebabkan terkena petir.	4	4	16
4	Perangkat DRC yang masih berada pada ruang yang sama dengan data center dan serve saat terjadi bencana.	Jika terjadi bencana pada ruang server dan data center, maka DRC dan file backup mengalami bencana yang sama sehingga tidak mampu mengembalikan informasi dan sistem beroperasi kembali.	4	4	16
5	Sistem operasi yang rentan dengan gangguan virus dan meningkatnya penyebaran virus melalui email, tanpa didukung oleh perangkat antivirus yang cukup handal, dapat menimbulkan kerusakan file, dan kehilangan file data.	Sistem operasi yang rentan dengan penyebaran virus, dapat berpotensi merusak informasi dan mengganggu jaringan komputer perusahaa.	4	4	16
6	Penggunaan firewall hanya pada sisi luar DMZ saja, berpotensi terbukanya wilayah server dari gangguan yang berasal dari dalam jaringan (lokal), karena area dalam DMZ tidak dilindungi firewall	Penyusupan dan gangguan yang berasal dari jaringan lokal dapat langsung masuk ke area DMZ dimana server berada, dan mengakses informasi dan sistem yang sensitif dan kritikal.	4	3	12
7	Tidak dilakukan pengujian terhadap file hasil backup sistem dan data.	Jika terjadi kehilangan data pada sistem utama, maka hasil backup tidak dapat direstore, terjadi kehilangan informasi.	4	3	12
8	Pegawai yang telah menguasai bisnis proses dan pengelolaan teknologinya, masih berstatus pegawai kontrak,	Berpotensi pegawai IT dapat keluar kapan pun dari perusahaan dan divisi IT kekurangan pegawai terlatih.	3	3	9

Kecenderungan dan Dampak (2)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
9	Karyawan di divisi TI yang cenderung bergant-ganti, sehingga dengan teknologi yang dgunakan oleh perusahaan, membutuhkan keterampilan dan pengetahuan yang cukup, agar dapat melakukan monitoring dan pemeliharaan terhadap sistem yang ada.	Karyawan pengganti atau baru tidak mampu menguasai teknologi perusahaan secara cepat, sehingga proses monitoring dan pemeliharaaan sistem menjadi lambat dan terhambat.	3	3	9
10	Terjadi kesalahan input data pada aplikasi di lapangan, dan tidak terdapat prosedur tetap dalam pelaporan dan verifikasi kesalahan tersebut.	Kesalahan input data tersebut jika tidak diverifikasi dan dikoreksi secara cepat, menyebabkan waktu layanan menjadi lama, dan akan menurunkan kepercayaan konsumen terhadap perusahaan.	3	3	9
11	Tidak dilakukannya pencatatan yang sistematis terhadap kejadian-kejadian gangguan keamanan yang terjadi,	Perusahaan tidak akan bisa menyadari kelemahan/kerawanan sistem yang dimiliki, menyebabkan kelemahan tersebut diketahui orang, yang akan mengganggu keamanan informasi.	3	3	9
12	Jika perusahaan memiliki karyawan baru tidak akan pernah mengetahui tentang kebijakan tentang keamanan informasi, karena aturan yang tidak tertulis dan tidak disosialisasikan dengan baik.	Kecerobohan dan kesalahan yang dilakukan karyawan, sehingga menyebabkan gangguan keamanan informasi.	3	3	9
13	Aplikasi yang dibangun dengan platform DBMS yang berbeda dan tidak memenuhi standard keamanan informasi pada aplikasi.	Integrasi data yang sulit, bisa disebabkan oleh aplikasi yang dibangun oleh pihak luar, yang tidak memperhatikan integrasi antar data pada aplikasi-aplikasi tersebut, sehingga ketersediaan data secara cepat dan lengkap menjadi sulit dicapai.	3	3	9
14	Modifikasi informasi dan pencurian informasi melalui komputer yang tidak mengaktifkan keamanan dekstop, saat pemiliknya tidak berada ditempat.	Terjadinya pengamblan, modifikasi dan kehilangan informasi file yang sensitif dan kritikal pada PC tersebut.	3	3	9

Kecenderungan dan Dampak (3)

No	Vulnerability	Threat	Likelihood Level	Impact Level	Ranking
15	Tidak dilakukan pemeliharaan terhadap perangkat pendukung yang kritikal secara rutin dan berkala, seperti pendingin ruangan pada ruang server dan listrik dengan gensetnya.	Pemeliharaan yang tidak dilakukan secara rutin dan berkala terhadap perangkat pendukung, seperti pendingin ruangan, dapat menyebabkan kerusakan secara mendadak, sehingga akan mengganggu terutama ruang yang kritikal seperti data center dan ruang server.	3	3	9
16	Informasi yang sensitif (rahasia) dapat dilakses dan dicuri oleh orang yang tidak berhak, karena informasi dilindungi oleh teknologi enkripsi pada informasi tersebut.	Informasi sensitif yang dibaca oleh orang yang tidak berhak, akan menyebabkan menurunnya kepercayaan konsumen terhadap perusahaan.	3	3	9
17	Tidak adanya kebijakan khusus yang mewajibkan karyawan untuk mengaktifkan firewall pada komputernya masing-masing.	Tidak diaktifkannya PC firewall, dapat memudahkan masuknya akses yang tidak terotorisasi, sehingga dapat menyebabkan hilangnya informasi, atau modifikasi dan kerusahakan sistem dan informasi.	3	3	9
18	Penggunaan aplikasi dan transaksi informasi yang terus bertambah, tidak terukur secara 19baik, sehingga sulit mengetahui kinerja dan beban sistem saat ini.	Kinerja sistem aplikasi dan transaksi data dapat menurun dan mati tiba-tiba, karena tidak pernah terukur secara baik penambahan beban dari waktu ke waktu.	2	3	6
19	Operator yang berstatus kontrak, berjumlah cukup banyak, dengan penugasan harian, cenderung rentan dengan penyalahgunaan.	Setiap operator diberikan otentikasi dan otorisasi dalam menggunakan aplikasi dan infirmasi, jika tidak diawasi secara baik, dapat berpotensi menjadi insiders yang mengganggu keamanan informasi.	2	3	6

15. Penilaian Risiko

Risk Scale and Necessary Actions

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

Identifikasi Tingkat Risiko (1)

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

Identifikasi Tingkat Risiko (2)

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

Analisis Kuantitatif pada Risiko akibat Gangguan Petir

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