

Tugas Kuliah

Proteksi dan Teknik Keamanan Sistem Informasi

Kelompok 72 Rumah Makan Saung Garing

Kelompok Saung Garing

Rumah Makan Sunda



Henry Aza Widjaja Y. – 7203010197

Kartini Slamet – 7203010278

Zaidan Rahmad - 7203010472

Magister Teknologi Informasi

Universitas Indonesia

Desember 2004

Daftar Isi

I. Profil Perusahaan.....	5
I.I. Latar Belakang.....	5
I.II. Struktur organisasi.....	6
I.III. Sistem penggajian karyawan.....	9
I.IV. Sistem Pengoperasian.....	9
I.V. Konfigurasi komputer dan portofolio aplikasi.....	10
I.VI. Denah lokasi kantor pusat dan cabang.....	12
II. Tujuan dan Lingkup.....	14
III. Access control system.....	15
III.I. Tujuan.....	15
III.II. Penerapan.....	15
I.I.A. <i>Access control system</i> pada aplikasi mesin cash register di cabang.....	15
I.I.B. <i>Access control system</i> pada di kantor pusat.....	15
I.I.C. Ringkasan pengawasan akses ke sistem pada restoran saung garing.....	17
IV. Telecommunication dan Network Security.....	18
IV.I. Tujuan.....	18
IV.II. Penerapan.....	18
V. Security Management Practices.....	19
V.I. Tujuan.....	19
V.II. Penerapan.....	19
V.II.A. Identifikasi Aset pada restoran saung garing.....	19
V.II.B. Information Asset valuation pada restoran saung garing.....	19
V.II.C. Jenis-jenis ancaman terhadap restoran saung garing.....	19
V.II.D. Penerapan pengawasan dan kontrol pada restoran saung garing.....	20
VI. Application dan Development security.....	21
VI.I. Tujuan.....	21
VI.II. Penerapan.....	21

VII. Cryptography.....	22
VII.I. Tujuan.....	22
VII.II. Penerapan.....	22
VIII. Security architecture and model.....	23
VIII.I. Tujuan.....	23
VIII.II. Penerapan.....	23
IX. Operations security	24
IX.I. Tujuan	24
IX.II. Penerapan.....	24
X. Disaster Recovery and Business Continuity plan	26
X.I. Tujuan	26
X.II. Penerapan	26
XI. Laws, Investigations and Ethics	28
XI.I. Tujuan	28
XI.II. Penerapan.....	28
XII. Physical Security	29
XII.I. Tujuan.....	29
XII.II. Penerapan.....	29
XIII. Audit and assurance.....	30
XIII.I. Tujuan.....	30
XIII.II. Penerapan.....	30

Daftar Tabel

Tabel I.1 Komposisi jumlah karyawan di kantor pusat	7
Tabel I.2 Komposisi jumlah karyawan di kantor cabang.....	7
Tabel I.3 Tabel <i>segregation of duties matrix</i> untuk kantor pusat.....	8
Tabel I.4 Tabel <i>segregation of duties matrix</i> untuk kantor cabang	8
Tabel I.5. Daftar gaji karyawan Saung garing.....	9
Tabel I.6. Spesifikasi komputer Saung Garing.....	11
Tabel III.1. Portfolio aplikasi <i>office automation</i> Saung Garing	16
Tabel III.2. Ringkasan akses kontrol Saung Garing	17
Tabel V.1. Information asset valuation Saung Garing.....	19

Daftar Gambar

Gambar I.1 Struktur organisasi.....	6
Gambar I.2 Denah ruangan kantor pusat.....	12
Gambar I.3 Denah ruangan kantor cabang.....	13

I. Profil Perusahaan

I.I. Latar Belakang

Restoran " Saung Garing", adalah restoran makanan sunda dan mempunyai enam lokasi di pusat kota Bandung yang terdiri dari satu restoran yang berlokasi di kantor pusat dan lima lainnya adalah restoran cabang. Setiap restoran mempunyai manager cabang yang bertanggung jawab penuh terhadap operasional pada lokasi tersebut. Restoran Saung Garing beroperasi penuh dari hari Senin sampai dengan hari Minggu, rata-rata dari jam 10.00 pagi sampai jam 10.00 malam.

Setiap cabang memiliki dapur sendiri yang akan menyediakan menu makanan yang sudah ditentukan oleh restoran pusat. Semua bahan-bahan baku makanan seperti beras, bumbu, udang, ikan, cumi, sayur-sayuran dan sebagainya di kirim dari kantor pusat setiap harinya, termasuk kebutuhan sehari-hari seperti *tissue*, sendok, garpu, piring, lap dsb. Demikian juga dengan pengadaan barang-barang keperluan restoran seperti furniture, freezer dan sebagainya di lakukan semua oleh kantor pusat. Untuk memenuhi kebutuhan sehari-hari pada setiap cabang, kantor pusat menyediakan 3 unit mobil box yang masing-masing-masing akan melayani pembelian dan pengangkutan barang-barang kebutuhan ke masing-masing kantor cabang.

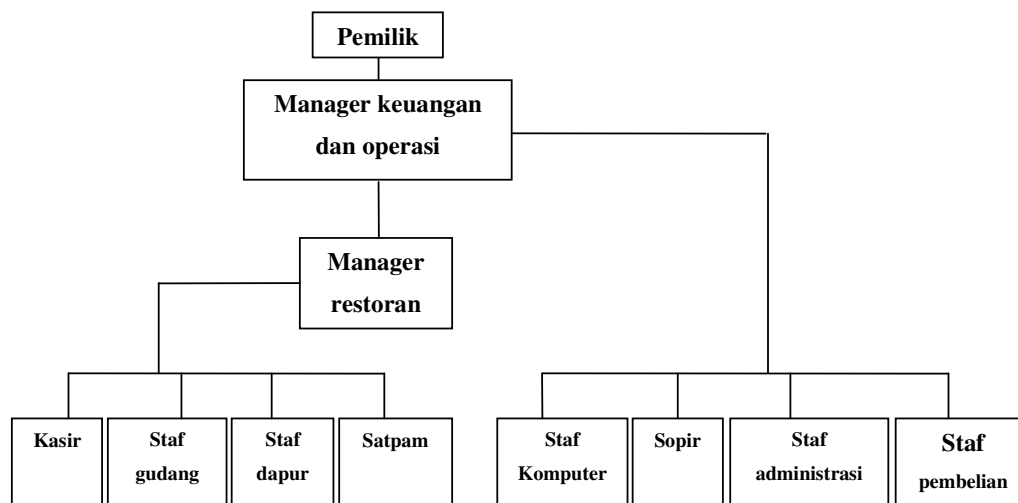
Rata-rata penghasilan setiap hari per cabang Rp 2.500.000, sementara rata-rata biaya yang dikeluarkan per bulan per cabang untuk bahan baku adalah Rp 25.000.000,00. biaya operasional (listrik, keamanan, air dsb) Rp 1.000.000,00.

Kantor pusat merupakan lokasi dengan omzet terbesar dengan rata-rata penghasilan per hari Rp 5.000.000,00. Sementara rata-rata pengeluaran per bulan di kantor pusat lebih kurang 2 kali pengeluaran per bulan kantor cabang. Kantor pusat sekaligus menjadi pusat pengendalian bahan baku makanan dan kebutuhan sehari-hari semua kantor cabang.

Sementara aset yang terlihat dari usaha ini adalah 6 buah gedung berikut isi serta lahan restoran (pusat dan cabang), 3 buah mobil operasional, dan alat-alat administrasi kantor (komputer, meja, kursi dan lemari).

I.II. Struktur organisasi

Dalam menjalankan bisnisnya, maka restoran saung garing membutuhkan beberapa tenaga kerja untuk mengoperasikan bisnis dari restoran saung garing. Oleh karena itu manajemen atau pemilik restoran saung garing telah menyusun suatu struktur organisasi yang diharapkan dapat menunjang bisnis yang sedang dijalankan. Berikut ini adalah gambar struktur organisasi restoran saung garing:



Gambar I.1 Struktur organisasi

Komposisi antara jumlah karyawan di kantor pusat dengan di kantor cabang berbeda, dan masing-masing jabatan mempunyai tugas dan tanggungjawab yang berbeda-beda pula.

Jumlah karyawan di masing-masing cabang sekitar 16 orang, terdiri dari 1 orang manajer cabang yang akan bertanggung jawab terhadap operasional dan keuangan sehari-hari, 1 orang kasir yang akan bertanggung jawab pada proses transaksi dengan

pelanggan, 4 staf bagian dapur yang akan bertanggung jawab pada proses pembuatan pesanan, 1 staf bagian gudang dan persediaan, 7 orang pelayan yang akan membantu dalam melayani pesanan-pesanan pelanggan, dan 2 orang satpam yang bertanggung jawab 7x24 secara bergantian mengamankan setiap cabang.

Sementara itu di kantor pusat jumlah karyawan jauh lebih banyak yaitu sekitar 38 orang yang terdiri dari 1 orang manager operasional dan keuangan pusat yang akan bertanggung jawab untuk seluruh operasional dan keuangan di semua kantor cabang, 1 orang manager restoran yang hanya bertanggung jawab penuh pada operasi restoran pusat, 1 orang kasir yang akan menerima transaksi dari pelanggan, 8 staf bagian dapur yang bertugas menyediakan pesanan pelanggan, 1 staf bagian gudang, 14 orang pelayan, dan 3 satpam. Selain itu ditambah dengan 2 staf administrasi, 1 staf bagian komputer, 3 orang staf pembelian, dan 3 orang sopir.

Secara ringkasnya komposisi jumlah karyawan di kantor pusat dapat dilihat pada tabel berikut:

Jabatan	Jumlah personil	Nama
Manajer operasional dan keuangan	1	A1
Manajer restoran	1	A2
Kasir	1	A3
Staf dapur	8	A4 s/d A11
Staf gudang	1	A12
Pelayan	14	A13 s/d 26
Satpam	3	A27 , A28, A29
Staf administrasi	2	A30, A31
Staf komputer	1	A32
Staf pembelian	3	A33, A34, A35
Sopir	3	A36, A37, A38

Tabel I.1 Komposisi jumlah karyawan di kantor pusat

Sedangkan komposisi jumlah karyawan di kantor cabang dapat dilihat pada tabel berikut ini:

Jabatan	Jumlah personil	Nama
Manajer cabang	1	B1
Kasir	1	B2
Staf dapur	4	B3, B4, B5, B6
Bagian gudang dan persediaan	1	B7
Pelayan	7	B8 s/d B14
Satpam	2	B15, B16

Tabel I.2 Komposisi jumlah karyawan di kantor cabang

Selain itu restoran saung garing juga membuat suatu pembagian tugas dan tanggungjawab baik untuk kantor pusat maupun kantor cabang yang disebut sebagai *segregation of duties matrix*. Tabel *segregation of duties matrix* untuk kantor pusat dapat dilihat pada tabel berikut.

Nama	Jabatan	Tugas	Operasional	Keuangan	Transaksi	Melayani pelanggan	Memasak	Inventori	Administrasi	Pemeliharaan komputer	Pengadaan barang	Mengantar barang	Menjaga keamanan
A1	Manajer operasional dan keuangan		X	X									
A2	Manajer restoran		X		✓	✓							
A3	Kasir				X								
A4 s/d A11	Staf dapur						X						
A12	Staf gudang							X					
A13 s/d 26	Pelayan					X							
A27 , A28, A29	Satpam												X
A30, A31	Staf administrasi								X				
A32	Staf komputer									X			
A33, A34, A35	Staf pembelian										X		
A36, A37, A38	Sopir											X	

Keterangan	Sifat
X	Mandatory
✓	Optional

Tabel I.3 Tabel *segregation of duties matrix* untuk kantor pusat

Sedangkan tabel *segregation of duties matrix* untuk kantor cabang dapat dilihat pada tabel berikut:

Nama	Jabatan	Tugas	Operasional	Keuangan	Transaksi	Melayani pelanggan	Memasak	Inventori	Administrasi	Pemeliharaan komputer	Pengadaan barang	Mengantar barang	Menjaga keamanan
A1	Manajer cabang		X	X		✓		✓	X				
A2	Kasir				X								
A3	Staf dapur						X						
A4 s/d A11	Bagian gudang dan persediaan							X			X		
A12	Pelayan					X							
A13 s/d 26	Satpam												X

Keterangan	Sifat
X	Mandatory
✓	Optional

Tabel I.4 Tabel *segregation of duties matrix* untuk kantor cabang

I.III. Sistem penggajian karyawan

Pihak manajemen restoran saung garing juga telah membuat suatu standar penggajian karyawan baik untuk kantor pusat maupun kantor cabang. Standar penggajian karyawan dapat dilihat pada tabel berikut:

Manajer operasional dan keuangan	Rp5,000,000
Manager cabang	Rp3,500,000
Kasir	Rp800,000
Pelayan	Rp500,000
Staf bagian dapur	Rp800,000
Staf bagian gudang	Rp500,000
Satpam	Rp800,000
Staf administrasi	Rp800,000
Staf Komputer	Rp1,000,000
Staf pembelian	Rp800,000
Sopir	Rp800,000

Tabel I.5. Daftar gaji karyawan Saung garing

I.IV. Sistem Pengoperasian

Setiap order pemesanan makanan akan di buat rangkap dua , yaitu satu copy di simpan bagian dapur dan satu copy oleh kasir. Setiap akhir hari kasir akan menghitung uang hasil penjualan yang dicocokkan dengan total uang yang dihasilkan dari mesin cash register. Setiap lokasi mempunyai seperangkat telepon, *fax*, dan *cash register* yang dapat menghasilkan data *digital* berupa file text dari hasil proses transaksi. Setelah selesai mencocokkan data kasir akan menyetorkan uang dan *file* dalam *floppy disk* kepada manager restoran. Manager restoran akan menyimpan uang cash tersebut kedalam *saving box* yang telah disediakan oleh kantor pusat pada setiap cabang. Setiap minggunya manager restoran akan menyetorkan uang pendapatan ke kantor pusat Sementara data transaksi dikirimkan pada setiap harinya.

Staf bagian gudang bertugas untuk mencatat semua bahan baku yang masuk dan keluar yang dibutuhkan oleh bagian dapur (bahan baku makanan) atau pelayan (kebutuhan piring, sendok, gelas, dsb). Staf ini juga mengawasi stok barang di gudang,

jika kemungkinan kurang. Setiap akhir hari staf bagian gudang akan melaporkan ke manajer cabang, apa saja bahan-bahan yang dibutuhkan keesokan harinya.

Setiap sore manajer cabang mengirimkan daftar pesanan bahan-bahan yang dibutuhkan untuk keesokan harinya melalui *fax* kepada staf bagian pembelian di kantor pusat. Berdasarkan pemesanan tersebut kantor pusat akan mengirimkan bahan-baku makanan tersebut ke cabang keesokan harinya. Pengangkutan bahan-baku merupakan tanggung jawab dari staf bagian pengangkutan.

Selain melaporkan bahan-bahan yang dibutuhkan pada akhir hari setiap manajer cabang melaporkan ringkasan hasil penjualan melalui *fax* ke kantor pusat. Setiap akhir minggu, semua data transaksi berupa struk penjualan dikirim ke kantor pusat, termasuk data absensi karyawan. Data-data ini dikirimkan ke staf bagian administrasi yang akan memasukkannya data ke dalam komputer.

Uang hasil penjualan setiap hari disimpan manajer cabang masing-masing di lemari tahan api dan seminggu sekali akan disetorkan kepada manajer keuangan di kantor pusat.

I.V. Konfigurasi komputer dan portofolio aplikasi

Aplikasi yang digunakan di cabang adalah:

1. Aplikasi cash register (stand alone POS)

Aplikasi yang mencatat semua transaksi di cabang.

Aplikasi ini menggunakan DOS 6.2 dan akan mencatat semua transaksi dalam bentuk *text file* yang dapat di *import* ke dalam *file excel*, lalu diekspresi dan disimpan 2 *copy* di mesin dan *floppy*. Selain itu mesin ini juga menghasilkan *hard copy* berupa salinan kertas struk transaksi.

Aplikasi yang digunakan di kantor pusat adalah :

1. *Inventory control*

Aplikasi digunakan untuk mengawasi dan mencatat perubahan stok barang di kantor pusat maupun di cabang. Aplikasi ini menggunakan RDBMS dengan MS Access 2000 dan berjalan pada *operating system windows 2000*.

2. Sistem penggajian karyawan dan data karyawan

- Aplikasi ini digunakan sebagai sistem penggajian karyawan dan data karyawan. *Database* yang digunakan MS Access 2000 dengan *operating system* windows 2000.
3. Aplikasi keuangan.
Aplikasi ini digunakan untuk menghitung keuntungan, termasuk pembayaran pajak. *Database* yang digunakan MS Access 2000, *operating system* windows 2000.
 4. Informasi *performance* cabang.
Aplikasi ini digunakan untuk melihat cabang mana yang menghasilkan keuntungan lebih banyak.
Database yang digunakan MS Access 2000 dengan *SQL function operating system* windows 2000.
 5. Office Automation
Aplikasi untuk menunjang kebutuhan sehari-hari operasional seperti membuat surat, membuat spreadsheet, dsb menggunakan MS Office.
 6. Email System
Aplikasi untuk menunjang kebutuhan sehari-hari untuk korespondensi.

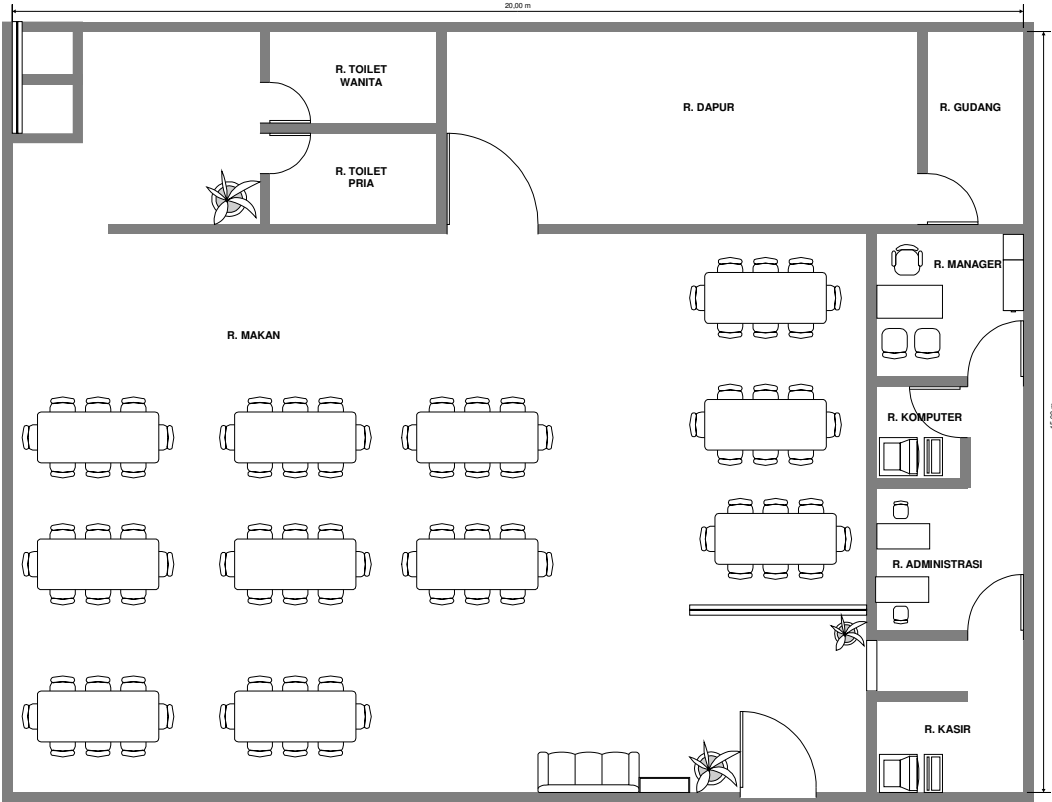
Pada kantor pusat terdapat tiga komputer yang terhubung lewat jaringan, dimana satu komputer terdapat di ruang staf administrasi, satu komputer untuk staf komputer dan satu lagi terdapat di ruang manajer keuangan. Sedangkan di kantor cabang tidak terdapat komputer. Semua database diletakkan di dalam *server*.

Spesifikasi masing-masing komputer				
		Ruang Keuangan	Ruang Staff Adminstrasi	Ruang Staff Komputer
Software	O/S	Windows 2000	Windows 2000	Windows 2000
	Applikasi	MS WORD 2000	MS WORD 2000	MS WORD 2000
		MS Power Point 2000	MS Power Point 2000	MS Power Point 2000
		MS Excel 2000	MS Excel 2000	MS Excel 2000
		MS ACCES 2000	MS ACCES 2000	MS ACCES 2000
		MS Outlook 2000	NAV Anti Virus	NAV Anti Virus
		NAV anti Virus		
Hardware	CPU	Pentium 4 1GHz	Celeron 500 MHz	Celeron 500MHz
	HDD	Maxtor 40 GB	Maxtor 20 GB	Maxtor 20 GB
		External Modem	NIC 100Mbps	NIC 100Mbps
		NIC 100Mbps		
		HUB		

Tabel I.6. Spesifikasi komputer Saung Garing

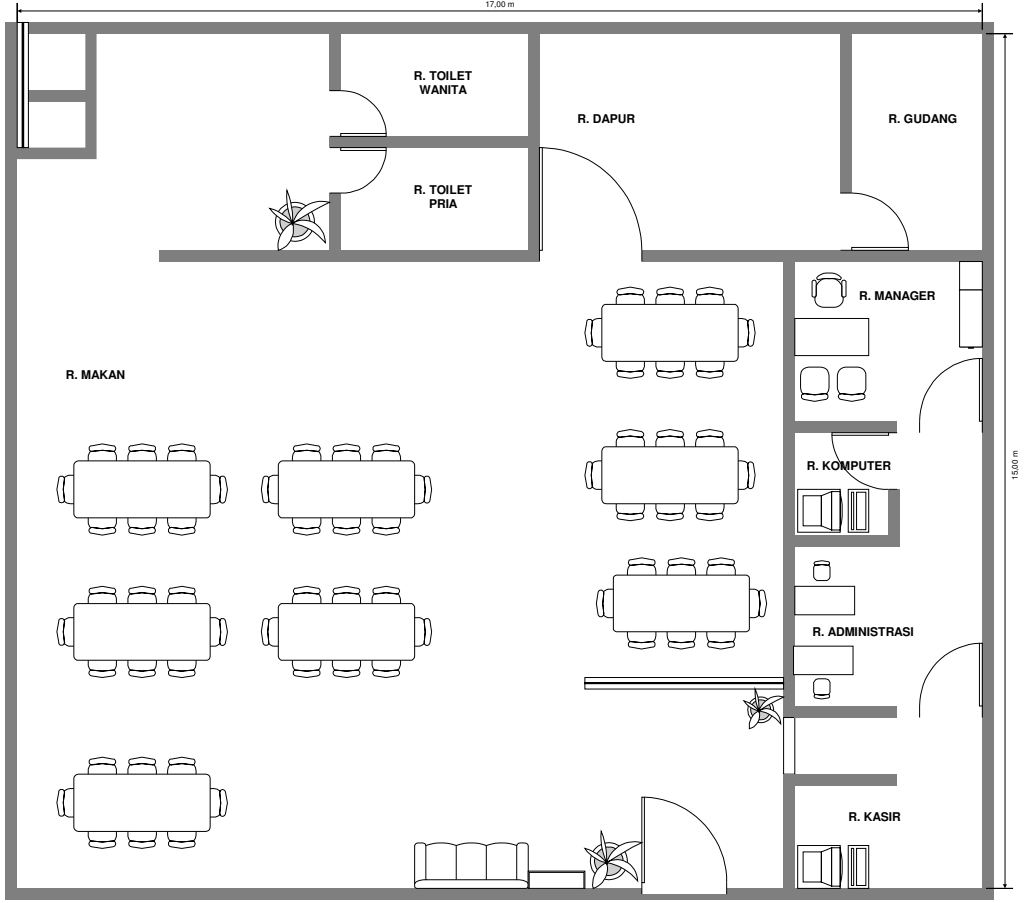
I.VI. Denah lokasi kantor pusat dan cabang

Agar lebih mudah memahami letak atau susunan ruangan kantor pusat dan cabang, maka diperlukan suatu denah ruangan. Denah ruangan dari kantor pusat dapat dilihat pada gambar berikut:



Gambar I.2 Denah ruangan kantor pusat

Sedangkan denah ruangan dari kantor cabang dapat dilihat pada gambar berikut:



Gambar I.3 Denah ruangan kantor cabang

II. Tujuan dan Lingkup

Tujuan tulisan ini adalah untuk memberikan rekomendasi keamanan sistem informasi untuk Restoran makanan sunda," saung garing", yang mencakup 11 aspek keamanan Sistem Informasi sebagai berikut :

1. Access Control System.
2. Telecommunication and Network Security.
3. Security Management Practices
4. Application and System Development Security
5. Cryptography
6. Security Architecture and Models
7. Operations Security
8. Disaster Recovery and Business Continuity Planning.
9. Laws, Investigation, and Ethics
10. Physical Security
11. Audit and Assurance

III. Access control system

III.I. Tujuan

Tujuan dari lingkup *access control system* adalah untuk menentukan mekanisme dan metode yang dipergunakan manajemen Saung Garing untuk mengawasi informasi apa yang boleh diakses *user*, termasuk apa yang boleh dilakukan setelah otentikasi dan otorisasi dan juga termasuk pemantauannya.

III.II. Penerapan

I.I.A. *Access control system* pada aplikasi mesin cash register di cabang

1. Setiap cabang hanya mempunyai dua orang yang berwenang untuk mengoperasikan mesin cash register, yaitu: kasir dan manajer cabang. Manajer cabang merupakan backup dari kasir, jika kasir tidak hadir.
2. Akses ke mesin cash register harus menggunakan user id dan password.
3. Akses kasir hanya terbatas pada *data entry* dan tidak bisa melakukan koreksi. Jika terjadi kesalahan, hanya manajer cabang yang berhak melakukan koreksi dengan memasukan *user id* dan *password*. Manajer cabang mempunyai akses penuh terhadap pengoperasian mesin cash register di cabangnya. Manajer cabang tidak mempunyai akses untuk delete data yang telah dimasukan tetapi hanya melakukan *reversal*.
4. Semua *password* dan *user id* di mesin *cash register* di buat oleh manajer keuangan dari kantor pusat saat pertama kali mesin di *install*.
5. Semua data transaksi terekam di dalam mesin *cash register* dalam bentuk *hardcopy (roll-tape)* dan juga didalam *text file* di *hard disk*. Akses ke *text file* hanya diperbolehkan untuk manajer cabang.

I.I.B. *Access control system* pada di kantor pusat

Pembatasan akses ke beberapa informasi di kantor pusat adalah sebagai berikut:

1. Aplikasi *Inventory Control*

Aplikasi inventory control hanya bisa diakses oleh staf administrasi dan manajer keuangan. Hak akses untuk staf administrasi adalah *create, read, update*. Sedangkan manajer keuangan hak aksesnya adalah *full access (Create, Read, Update, Delete)*.

2. Aplikasi keuangan

Aplikasi ini hanya bisa diakses oleh staf administrasi dan manajer keuangan dengan hak akses *create* dan *read*. Setiap ada koreksi hanya bisa dilakukan dengan cara melakukan *reverse* terhadap data kesalahan.

3. Aplikasi sistem penggajian karyawan

Aplikasi ini hanya bisa diakses penuh oleh manajer keuangan.

4. Aplikasi Performa cabang

Aplikasi hanya bisa diakses oleh manajer keuangan.

5. *Office Automation*

Aplikasi dapat diakses oleh semua pengguna komputer.

Portfolio Aplikasi		
Ruang Keuangan	Ruang Staff Adminstrasi	Ruang Staff Komputer
MS WORD 2000	MS WORD 2000	MS WORD 2000
MS Power Point 2000	MS Power Point 2000	MS Power Point 2000
MS Excel 2000	MS Excel 2000	MS Excel 2000
MS ACCES 2000	MS ACCES 2000	MS ACCES 2000
MS Outlook 2000	NAV Anti Virus	NAV Anti Virus
NAV anti Virus		

Tabel III.1. Portfolio aplikasi *office automation* Saung Garing

6. *Email system*

Aplikasi dapat diakses oleh manajer keuangan dari komputer yang berlokasi diruangan manajer keuangan.

7. Akses ke komputer

Setiap user harus mempunyai *username* dan *password* untuk dapat mengakses ke komputer begitu pula saat akan mengakses *database*, staf administrasi dan manajer keuangan harus mempunyai *password*. Akses ke komputer operasional atau *production* hanya diperbolehkan untuk staf administrasi dan manajer keuangan. Staf komputer tidak diperbolehkan. Staf bagian komputer hanya diperbolehkan akses ke komputer untuk pengembangan dan administrasi sistem sistem saja.

I.I.C. Ringkasan pengawasan akses ke sistem pada restoran saung garing

	Kasir cabang	Manajer cabang	Staf administrasi	Manajer keuangan	Staf komputer
Akses ke komputer / PC					
Cash register cabang	Ya	Ya	Tidak	Tidak	Tidak
Bagian Administrasi	Tidak	Tidak	Ya	Ya	Tidak
Bagian komputer	Tidak	Tidak	Tidak	Ya	Ya
Bagian Manajer keuangan	Tidak	Tidak	Ya	Ya	Tidak
Aplikasi (production)					
Inventory control			Create, Read, update	Full access	Tidak
Keuangan			Create, Read	Create, Read	Tidak
Penggajian pegawai			Tidak	Full access	Tidak
Performa cabang			Tidak	Full access	Tidak
Cash register	Create, Read	Create, Read, Koreksi	Tidak	System administrator	Read only
Aplikasi (pengembangan)			None	Full access	Full access
Database			Create, Read, Update	System administrator	Read only
Server				System administrator	

Tabel III.2. Ringkasan akses kontrol Saung Garing

IV. Telecommunication dan Network Security

IV.I. Tujuan

Tujuan dari lingkup *Telecommunication dan Network security* adalah untuk menerapkan aspek keamanan yang terkait untuk jaringan komputer atau telekomunikasi.

IV.II. Penerapan

Restoran saung garing mempunyai satu jaringan LAN di kantor pusat, sistem keamanan jaringan cukup dengan menggunakan *password* untuk dapat masuk ke komputer yang lain. Selain itu untuk folder yang di share juga harus diberi *password*.

Untuk akses ke internet diperbolehkan dengan menggunakan modem *dial up* dan modem tersebut dikonfigurasi agar modem hanya dapat melakukan koneksi ke internet secara manual, di mana *user* yang ingin menggunakan modem tersebut harus memasukkan *userid* dan *password*.

Selain itu untuk menghindari penyalahgunaan alat, maka modem hanya ada di komputer yang berlokasi di manajer keuangan. Sebagai informasi tambahan, tidak ada pengiriman data secara elektronik dari cabang ke kantor pusat atau sebaliknya.

Untuk proteksi jaringan dari serangan virus, pada setiap komputer harus dipasang antivirus, dan user yang ingin memasukkan data dari luar harus melakukan *scanning* terhadap media yang digunakan. Selain itu antivirus pada masing-masing komputer harus *diupdate* secara berkala dari komputer manajer keuangan setiap hari, dengan tujuan apabila ada virus baru maka virus tersebut dapat segera dideteksi.

V. Security Management Practices

V.I. Tujuan

Tujuan dari lingkup *Security Management Practices* adalah untuk menerapkan cara identifikasi aset perusahaan yang berupa informasi berikut cara terbaik untuk menentukan tingkat keamanannya, serta anggaran yang patut untuk implementasi keamanannya.

V.II. Penerapan

V.II.A. Identifikasi Aset pada restoran saung garing

Aset tangible (hardware dan ruangan)

Mesin cash register

Komputer

Aset intangible (Software dan data)

Informasi data inventori

Informasi data keuangan

Informasi data pegawai

Informasi data performa cabang

V.II.B. Information Asset valuation pada restoran saung garing

Information Asset valuation				
	Data keuangan	Data pegawai	Data inventori	Data performa cabang
Confidentiality	Rahasia	Rahasia	Tidak Rahasia	Rahasia
Integrity	Akurat	Akurat	Tidak Akurat	Akurat
Availability	Penting	Penting	Tidak penting	Tidak penting

Tabel V.1. Information asset valuation Saung Garing

V.II.C. Jenis-jenis ancaman terhadap restoran saung garing

1. Penghapusan (*destruction*), misalnya : penghapusan data-data penjualan secara tidak sengaja, bencana banjir, kebakaran, kerusakan, listrik mati atau virus.
2. Pencurian (*theft/disclosure*), misalnya : data penjualan atau rugi laba dari saung garing terungkap kepada semua pegawai
3. Pengubahan (*modification*) misalnya : secara tidak sengaja mengubah nilai gaji dalam sistem penggajian pegawai
4. Penipuan (*fraud*) misalnya : mengubah nilai gaji dalam sistem penggajian pegawai secara tidak sah, mengubah data penjualan secara tidak sah.

V.II.D.Penerapan pengawasan dan kontrol pada restoran saung garing

Preventive control / pencegahan

1. Pemisahan tugas kasir, manajer cabang, staf administrasi, staf komputer dan manajer keuangan.
2. Melakukan enkripsi semua data yang bersifat rahasia
3. Semua komputer harus di *install anti virus* versi terakhir setiap hari
4. Setiap karyawan tidak boleh meninggalkan data *confidential* di tempat yang mudah dijangkau oleh orang yang tidak berkepentingan setelah jam kerja.
5. Penerapan *Business Continuity Plan* (Akan dibahas di bab BCP)

Detective control /pendeteksian

1. Pengecekan ulang pada akhir hari dan minggu oleh bagian administrasi kantor pusat terhadap data penjualan
2. Inspeksi secara berkala terhadap kas cabang oleh manajer keuangan
3. Semua data penjualan disimpan dalam bentuk *roll-tape* dan didalam *hard disk*, akses ke data ini juga dibatasi hanya untuk manajer cabang dan staf kantor pusat.

Corrective control / memperkecil dampak ancaman

1. Melakukan prosedur *backup* setiap hari terhadap data cabang
2. Data-data didalam media *backup* harus disimpan ditempat yang aman dari kebakaran, banjir dan orang yang tidak berkepentingan

VI. Application dan Development security

VI.I. Tujuan

Mempelajari berbagai aspek keamanan dan kontrol-kontrol yang terkait pada pengembangan sistem informasi.

VI.II. Penerapan

Aplikasi yang akan digunakan atau diimplementasikan harus selalu mendapat persetujuan dari pemilik atau manajer keuangan. Jika ada masalah dengan salah satu aplikasi tersebut, staf bagian komputer akan dipanggil untuk memberikan bantuan, dalam kondisi sehari-hari perubahan terhadap aplikasi dilakukan di komputer terpisah dari komputer operasional, yang digunakan khusus untuk *troubleshooting* atau pengembangan sistem. Staf bagian komputer tidak mendapat akses ke komputer *production* atau operasional. Setiap aplikasi disimpan didalam media seperti disket atau CDROM. Versi control juga diterapkan dengan selalu menyimpan program dengan minimum 2 versi terakhir.

VII. Cryptography

VII.I. Tujuan

Menerapkan metode dan teknik penyembunyian data menggunakan kriptografi untuk informasi yang masuk kategori *confidential*.

VII.II. Penerapan

Saung garing mengharuskan data, terutama data laporan keuangan yang dikirim melalui media dan bersifat *confidential* harus di enkripsi. Dalam hal ini data keuangan dari cabang yang dikirim lewat disket dienkripsi dengan menggunakan PGP.

Proses enkripsi ini akan dibantu oleh staf lain, yaitu staf komputer untuk melakukan enkripsi.

VIII. Security architecture and model

VIII.I. Tujuan

Menerapkan konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman pada saung garing.

VIII.II. Penerapan

Agar dapat mendukung *policy* dan *procedure* yang ada, maka menentukan security architecture dan security model sangatlah penting.

Untuk *security architecture*, terbagi menjadi dua bagian, yaitu secara logikal dan fisikal. Security secara logikal terbagi menjadi dua yaitu security oleh sistem operasi dan security oleh sistem aplikasi, di mana security oleh sistem operasi merupakan security paling dasar, dan didukung lapisan di atasnya yang mendukung security sistem operasi, yaitu security oleh sistem operasi. Security secara logikal ini mirip dengan *security architecture* ring, di mana lapisan yang lebih luar melakukan proteksi terlebih dahulu dari *intruder*.

Sedangkan *security architecture* secara fisikal, adalah melakukan *security* dengan cara melakukan proteksi terhadap *I/O device* yang terdapat di komputer *server*, misalnya mengunci komputer *server* agar *I/O device* tidak dapat digunakan oleh orang yang tidak berkepentingan.

Untuk *security model*, adalah dengan menggunakan *security model matrix*, atau yang lebih dikenal dengan nama *access matrix model*. Desain terhadap *security model* (*access matrix model*) sudah dilakukan, dan dapat dilihat pada tabel “Ringkasan pengawasan akses ke sistem pada restoran saung garing” pada bab 3, yaitu *access control system*.

IX. Operations security

IX.I. Tujuan

Menerapkan teknik-teknik kontrol pada operasi personalia Sistem Informasi, sistem informasi dan perangkat keras.

IX.II. Penerapan

Saung garing menerapkan *operations security* untuk meningkatkan keamanan informasi atau datanya. Penerapan *information security* dari saung garing adalah sebagai berikut:

1. *Least priviledge/need to know basis*

Misalnya pada bab access control terlihat bahwa akses ke komputer tidak diberikan kepada semua orang, tetapi diberikan kepada pengguna komputer sesuai dengan fungsinya.

2. *Separation/segregation of duties*

Disini terlihat adanya pemisahan tugas yang jelas antara staf bagian komputer dengan misalnya staf administrasi dengan manajer keuangan. Staf bagian komputer tidak mempunyai akses ke *database production*, tetapi terbatas hanya pada komputer untuk pengembangan sistem saja.

3. *Change Management control*

Semua perubahan sistem harus disetujui oleh manajer keuangan, dan semua modifikasi program harus dites sebelum di implementasikan ke *production*. Pada bab *Application and Development Security* terlihat adanya pengawasan terhadap semua aplikasi yang running di Saung garing. Aplikasi masuk *production* harus dengan seijin manajer keuangan.

4. *Record Retention*

Semua data Saung garing harus di backup setiap hari oleh staf administrasi dan/atau manajer keuangan. Data didalam server atau komputer paling lama selama 1 bulan, lalu disimpan di disket. Jika diperlukan dapat di *restore* kembali.

5. *Email security*

Saung garing tidak mempunyai email server, sehingga security tidak dibahas pada tugas ini.

X. Disaster Recovery and Business Continuity plan

X.I. Tujuan

Menerapkan perencanaan DRP yang baik agar aktifitas bisnis saung garing dapat tetap berjalan meskipun terjadi gangguan atau bencana.

X.II. Penerapan

Pada bab *security management practices*, terlihat bahwa data keuangan dan data pegawai adalah dua data terpenting untuk saung garing dari segi *availability*. Sementara berdasarkan analisa, saung garing menghadapi ancaman ancaman sbb:

1. Penghapusan (*destruction*), misalnya: penghapusan data-data penjualan secara tidak sengaja, bencana banjir, kebakaran, kerusakan, listrik mati atau virus.
2. Pencurian (*theft/disclosure*), misalnya: data penjualan atau rugi laba dari saung garing terungkap kepada semua pegawai.
3. Perubahan (*modification*), misalnya: secara tidak sengaja mengubah nilai gaji dalam sistem penggajian pegawai.
4. Penipuan (*fraud*), misalnya: mengubah nilai gaji dalam sistem penggajian pegawai secara tidak sah, mengubah data penjualan secara tidak sah.

Berikut ini adalah langkah2 yang diambil oleh restoran saung garing dalam rangka memastikan kelangsungan bisnis tidak terganggu.

1. Ancaman Penghapusan (*destruction*)
 - a. Bencana banjir

Data diletakan ditempat yang kemungkinan tidak terkena banjir, termasuk backup data di kantor pusat dan mesin cash register di kantor cabang
 - b. Kebakaran
 - Saung garing mengharuskan setiap cabang mempunyai fire extinguisher didekat komputer operasional, dapur dan di dekat panel listrik.
 - Mengharuskan mempunyai backup data 1 minggu terakhir yang disimpan di lemari tahan api.
 - Data penjualan di kantor pusat menjadi backup data dari kantor cabang dengan selisih waktu 1 minggu.

- c. Kerusakan
Data dikirim ke kantor pusat minimum setiap minggu dan data transaksi disimpan dalam bentuk disket dan *hardcopy*.
 - d. Listrik mati
Semua komputer di kantor cabang maupun di kantor pusat diharuskan tersambung ke UPS
 - e. Virus
Semua komputer termasuk *server* diterapkan *software anti virus* dengan *update* setiap hari
2. Pencurian (*theft/disclosure*)
Tidak dibahas pada bab BCP, akan dibahas pada *physical security*.
 3. Pengubahan (*modification*)
Tidak dibahas pada bab BCP, tetapi pada *security management practices* dan akses kontrol.
 4. Penipuan (*fraud*)
Tidak dibahas pada bab BCP, tetapi pada *security management practices* dan akses kontrol

XI. Laws, Investigations and Ethics

XI.I. Tujuan

Mempelajari berbagai jenis aturan yang terkait dengan kejahatan komputer dan legalitas transaksi elektronik, serta membahas masalah etika dalam dunia komputer.

XI.II. Penerapan

Restoran Saung garing memberlakukan beberapa kebijakan-kebijakan sehubungan dengan legalitas transaksi elektronik dan copy right sbb:

1. Semua *software* yang dipakai adalah software asli dan bukan bajakan.
2. Semua staf terutama staf bagian komputer diharuskan menanda tangani peraturan untuk menjaga kerahasiaan sistem saung garing.
3. Semua staf terutama staf bagian komputer tidak diperbolehkan melakukan *copy software* keluar apalagi mengimplementasikan aplikasi tersebut tanpa seijin saung garing.

XII. Physical Security

XII.I. Tujuan

Menerapkan sistem kontrol untuk menghadapi berbagai ancaman terhadap fasilitas sistem informasi. Lingkup mencakup: *Physical access control (Guards, fences, keys and locks, badges, escorts, monitoring/detection system), environmental protection (power protection, water protection, fire detection, fire suppression, evacuation, environment monitoring/detection).*

XII.II. Penerapan

Untuk mencegah ancaman terhadap pencurian, saung garing menerapkan physical security sbb :

- Kantor harus dijaga oleh satpam selama 7 x 24 jam secara bergantian.
- Setiap tamu yang ingin masuk keruang komputer harus memakai *badge visitor*.
- Ruang tempat akses data/komputer/mesin *cash register* harus terletak di tempat yang tidak mudah dijangkau orang yang tidak berkepentingan.
- Kunci ruangan tempat penyimpanan data dan komputer disimpan oleh manajer keuangan, dan kunci duplikat disimpan oleh satpam.
- Ruang kasir/lokasi cash register di cabang tidak boleh di tempat publik dimana banyak orang lalu lalang. Juga jangan terlalu di depan, untuk menghindari perampokan atau kerusuhan.
- Backup data disimpan dan dikunci di lemari besi
- Untuk mencegah kerusakan komputer/mesin cash register, ruang tempat komputer, *server* dan mesin *cash register* berada harus dijaga suhu ruang dan humidity nya dan harus diletakan ditempat yang jauh dari kebocoran, dapur dsb

XIII. Audit and assurance

XIII.I. Tujuan

Menerapkan auditing sistem informasi terkait dengan masalah keamanan sistem informasi.

XIII.II. Penerapan

Secara periodik (6 bulan sekali) diadakan pengecekan terhadap aspek aspek keamanan sistem informasi di saung garing.

Staf yang melakukan pengecekan adalah manajer keuangan dan dibantu oleh satu staf yang independen dari pekerjaan sehari-hari. Biasanya pihak manajemen saung garing meminta salah satu manajer cabang melakukan pengawasan berkala kepada cabang lain dengan pengawasan manajer keuangan. Khusus untuk staf administrasi, pengecekan dilakukan sendiri oleh manajer keuangan.

Dalam melakukan audit terhadap sistem informasi, saung garing menggunakan tahapan-tahapan sebagai berikut:

1. *Tahap pengumpulan informasi dan perencanaan*

Pada tahapan ini, tim audit akan melakukan perencanaan kegiatan audit misalnya: identifikasi siapa yang akan menjadi tim audit sesuai dengan *technical skill* dan *resource* yang dibutuhkan, identifikasi lokasi atau lingkup perusahaan yang akan diaudit, identifikasi sumber informasi, dll.

Tahap selanjutnya pengumpulan informasi terhadap lingkup yang akan diaudit, misalnya: data data cabang yang akan di audit , hasil audit tahun lalu (jika pernah dilakukan audit pada tahun sebelumnya), dll.

2. *Obtain Understanding of Internal Control*

Setelah melakukan pengumpulan informasi dan membuat rencana audit, maka tahapan selanjutnya adalah melakukan pemahaman terhadap *control environment*, *control objective*, *control procedures* atau *activity*, dll.

Tahapan ini diperlukan agar tim audit dapat mengetahui kontrol apa saja yang ada di perusahaan tersebut untuk melindungi sistem informasi yang ada.

3. *Lakukan compliance test*

Pada tahapan ini dilakukan pengecekan apakah *policy* dan *procedure* yang ada sudah dilaksanakan dengan baik oleh karyawan dari perusahaan tersebut, dalam hal ini misalnya apakah akses ke mesin cash register memang hanya terbatas pada kasir dan manajer cabang saja. Apakah akses staf administrasi hanya terbatas pada aplikasi yang telah disetujui.

Selain itu pada tahapan ini juga akan dilakukan tahapan *test of segregation of duties*, dengan tujuan agar tim audit dapat melakukan penilaian apakah *policy* dan *procedure* yang ada dilaksanakan dengan adanya pembedaan tugas dan tanggungjawab antara karyawan yang satu dengan yang lain, misalnya apakah memang benar staf komputer tidak mendapat akses ke production.

4. *Lakukan Substantive Tests*

Setelah melakukan *compliance test*, perlu dilakukan *substantive test* agar dapat diketahui apakah *compliance* benar-benar telah dilakukan, dengan kata lain tim audit akan melakukan penyelidikan lebih lanjut dan mengumpulkan bukti-bukti. Contoh dari kegiatan ini adalah melakukan penyelidikan dan analisa terhadap *user group* yang terdapat di sistem operasi (misalnya Windows 2000 Server), lalu tim audit akan memeriksa apakah *user* yang ada sesuai dengan ketentuan yang telah ditetapkan oleh perusahaan, misalnya *user* biasa tidak boleh dimasukkan ke dalam *administrator user group*.

5. *Pengambilan kesimpulan*

Setelah melakukan pengecekan atau *substantive test*, maka tim audit harus membuat suatu dokumen, yang biasanya disebut *audit report* yang nantinya akan diberikan ke manajemen agar manajemen dapat mengetahui dan melihat resiko dan kelemahan apa yang ada di perusahaan tersebut.

Selain itu pada *audit report* juga terdapat rekomendasi terhadap penemuan-penemuan misal resiko, kelemahan, dll, agar manajemen juga dapat segera mengambil keputusan dari hasil rekomendasi tersebut.