BAB IV SIMPULAN DAN SARAN

4.1 Simpulan

Hasil simpulan yang dapat diambil dari analisis proses keamanan lokasi, manajemen operasi dan komunikasi serta pengendalian akses kontrol diantaranya :

1. PT.KAI telah menerapkan keamanan fisik dan lingkungan untuk melindungi aset informasi, namun masih kurangnya kepedulian organisasi dan pegawai terhadap aset tersebut, dikarenakan masih belum lengkapnya kebijakan dan prosedur yang ada.
2. PT.KAI telah melakukan proses operasi dan komunikasi namun perusahaan masih dalam tahap perencanaan untuk membuat kebijakan dan prosedur yang mengatur proses operasi dan komunikasi.
3. PT.KAI telah menjalakan proses pengendalian akses kontrol dengan baik, namun dalam penerapannya masih terdapat celah untuk melakukan modifikasi atau pengaksesan oleh pihak yang tidak berwenang karena kurangnya perhatian dari manajemen yang bertanggung jawab untuk melakukan pemantauan secara reguler dan belum adanya prosedur yang mengatur secara formal.

4.2 Saran dan Rekomendasi

Berdasarkan hasil analisis yang telah dilakukan di PT.KAI berikut adalah beberapa saran seusai dengan proses yang ada diantaranya adalah :

1. Keamanan fisik dan Lingkungan
    a. Perimeter keamanan fisik

       Pengendalian akses fisik terhadap sistem informasi dapat ditingkatkan lagi agar terlindungi dari akses pihak yang tidak berwenang.
    b. Pengendalian entri bersifat fisik

       pengendalian entri fisik terhadap sistem informasi dapat ditingkatkan lagi agar terlindungi dari akses pihak yang tidak berwenang.
    c. Mengamankan kantor, ruangan dan fasilitas

       Manajemen tingkat atas agar mendukung perancangan keamanan fisik terhadap aset informasi yang dimiliki dan menerapkannya.
    d. Perlindungan terhadap ancaman eksternal dan lingkungan

       Manajemen tingkat atas agar mendukung perancangan keamanan fisik terhadap aset informasi yang dimiliki dan menerapkannya.
    e. Bekerja diarea yang aman

       Harus tersedia pedoman untuk bekerja dalam perlindungan area yang aman.
    f. Area akses publik dan bongkar muat

       Harus dibuat prosedur tertulis agar lebih jelas instruksinya.
    g. Penempatan dan perlindungan peralatan

       Perlu ada prosedur tetap agar prosedur penempatan dan perlindungan peralatan dapat dijalankan dengan benar.
    h. Sarana Pendukung

penerapan sarana pendukung harus dikendalikan dengan menggunakan prosedur yang formal.

i. Keamanan kabel

Agar di beri instruksi jelas kepada pegawai untuk menjaga dan merawat kemanan kabel.

j. Pemeliharaan peralatan

seluruh pegawai harus diberi instruksi yang jelas mengenai pemeliharaan peralatan yang digunakannya agar tidak menghambat proses yang sedang berjalan.

k. Keamanan peralatan di luar lokasi

Agar setiap peralatan yang akan dibawa ke luar lokasi perusahaan di identifikasi terlebih dahulu dan di cek apabila akan kembali ke dalam lokasi perusahaan.

l. Pembuangan atau penggunaan kembali peralatan secara aman.

Agar setiap pegawai memiliki tingkat perhatian yang tinggi karena menyangkut data perusahaan.

m. Pemindahan barang

Tanggung jawab manajemen dan prosedur harus diterapkan untuk memastikan setiap peralatan dan informasi yang dibawa ke luar lokasi melalui proses yang benar.

2. Manajemen Komunikasi dan Operasi

a. Prosedur operasi terdokumentasi

Tanggung jawab manajemen dan prosedur harus diterapkan agar setiap proses yang berlangsung di perusahaan dapat di dokumentasikan dengan baik dan di pelihara.

b. Manajemen perubahan

Tanggung jawab manajemen dan prosedur harus diterapkan agar setiap proses yang berlangsung di perusahaan dapat di dokumentasikan dengan baik dan di pelihara.

c. Pemisahan tugas
d. Pemisahan fasilitas pengembangan, pengujian dan operasional
e. Pelayanan jasa

   Pengecekan terhadap layanan jasa dari pihak ketiga harus dilakukan secara regular untuk memastikan layanan yang diberikan oleh pihak ketiga sudah seusai dengan perjanjian
f. Pemantauan dan pengkajian data

   Pemantauan sebaiknya dilakukan secara regular dan berkala untuk mendapatkan hasil yang baik
g. Pengelolaan perubahan terhadap jasa pihak ketiga

   Agar prosedur dijalakan dengan benar.
h. Manajemen kapasitas

   Kebijakan mengenai manajemen kapasitas harus lebih disosialisasikan kepada sumber daya yang dimiliki perusahaan
i. Keberterimaan sistem

   harus tersedia prosedur pada sistem informasi yang baru, upgrade dan versi yang baru ditetapkan.
j. Perlindungan terhadap *malicious code*

   agar dibuat instruksi legal mengenai perlindungan terhadap *malicious code*
k. Perlindugnan terhadap *mobile code*

agar dibuat instruksi legal mengenai perlindungan terhadap mobile code

l. *Back-up* informasi

Agar dibuat prosedur yang jelas dan legal untuk melindungi data informasi yang dimiliki perusahaan

m. Pengendalian jaringan

Penerapan pengendalian jaringan harus di pertahankan atau di tingkatkan kembali

n. Keamanan layanan jaringan

Penerapan keamanan layanan jaringan harus ditingkatkan kembali

o. Manajemen media yang dapat dipindahkan

Agar setiap media yang akan dipindahkan didokumentasikan

p. Pemusnahan media

Pemusnahan media agar dilakukan untuk memastikan data atau informasi tidak jatuh ke pihak yang tidak berwenang

q. Prosedur penanganan informasi

Agar segera dibuat prosedur tersebut

r. Keamanan dokumentasi sistem

Agar segera dibuat prosedur tersebut

s. Kebijakan dan prosedur pertukaran informasi

Perusahaan harus memiliki prosedur pertukaran informasi

t. Perjanjian pertukaran

Agar segera dibuat prosedur tersebut

u. Pesan elektronik

Aturan pesan elektronik agar dititingkatkan kembali

v. Sistem informasi bisnis

Perusahaan agar membuat instruksi tersebut

w. *Electronic commerce*

harus tersedia instruksi legal mengenai *electronic commerce*

x. Transaksi *online*

harus terdapat instruksi jelas dan legal yang mengatur traksaksi *online*

y. Informasi yang tersedia untuk umum

Agar selalu me*maintenance* informasi yang tersedia untuk umum

z. *Log audit*

Agar perusahaan membuat instruksi yang jelas dan legal

aa. Pemantauan penggunaan sistem

Agar setiap pemantauan penggunaan sistem di pantau secara reguler

bb. Perlindungan informasi *log*

Agar perlindungan terhadap informasi *log* ditingkatkan agar tidak ada akses oleh pihak yang tidak berwenang

cc. *Log* administrator dan operator

Agar seluruh kegiatan administrator dan operator dapat terpantau secara reguler

dd. *Log* atas kesalahan yang terjadi

Agar setiap kesalahan yang terjadi dicatat dan di analisa untuk diambil tindakan

ee. Sinkronisasi penunjuk waktu

agar setiap waktu yang terdapat di sistem perusahaan dapat disinkronisasikan seluruhnya

3. Pengendalian Akses

a. Kebijakan pengendalian akses

   Harus tersedia prosedur untuk mengendalikan kebijakan pengendalian akses

b. Pendaftaran pengguna

   Harus tersedia prosedur yang mengendalikan hak hak akses pengguna

c. Manajemen hak khusus

   Penggunaan hak akses oleh pihak yang tidak berwenang harus diminimalisirkan

d. Manajemen *password* pengguna

   Pengguna harus dicegah untuk member *password* miliknya dengan pegawai lain

e. Tinjauan terhadap hak akses

   Pengendalian tinjauan hak akses harus dibuat agar dapat meninjau hak hak akses setiap pegawai

f. Penggunaan *password*

   Password agar di tetapkan ketentuannya agar sesuai dengan standar yang akan digunakan

g. Peralatan yang ditinggalkan oleh pengguna

   Manajer harus memastikan bahwa seluruh peralatan yang sudah ditinggalkan oleh penggunanya dapat dilindungi atau disimpan dengan baik dan benar

h. Kebijakan *clear desk and screen*

   Agar secepatnya dibuat kebijakan clear desk and screen

i. Kebijakan penggunaan layanan

   Agar setiap layanan yang diberikan untuk pengguna diberikan secara spesifik

j. Otentikasi pengguna untuk koneksi eksternal

Harus direncanakan membuat kebijakan otentikasi pengguna untuk koneksi eksternal

k. Identifikasi peralatan dalam jaringan

   manajemen agar lebih peduli terhadap kebijakan identifikasi peralatan dalam jaringan

l. Perlindungan terhadap *remote diagnostic* dan *configuration port.*

   Perlindungan *remote diagnostic* dan *configuration port* agar ditingkatkan kembali

m. Segregasi dalam jaringan

   Agar dibuat instruksi secara formal

n. Pengendalian koneksi jaringan

   Perluasan jaringan harus dibarengi dengan pengendalian koneksi jaringan sehingga ada yang mengatur secara formal

o. Pengendalian *routing* jaringan

   Prosedur harus diterapkan dan dibuat untuk memastikan kesesuaian dengan persyaratan yang dibutuhkan

p. Prosedur *log-on* yang aman

   Prosedur harus diterapkan dan dibuat untuk memastikan kesesuaian dengan persyaratan yang dibutuhkan

q. Identifikasi dan otentikasi pengguna

   Prosedur harus dibuat untuk membatasi dan mengatur pegawai yang memiliki user-id

r. Sistem manajemen *password*

   Apabila ingin memiliki prosedur ini harus membuat dulu sistem manajemen *password*

s. Pengguna sistem *utilities*

   Agar dibuat prosedur pengguna sistem utilities

t. Sesi *time out*

   Agar dibuat prosedur sesi *time out*

u. Pembatasan waktu koneksi

   Pengguna harus mematuhi aturan yang berlaku diperusahaan

v. Pembatasan akses informasi

   Kedepannya agar setiap pengguna memiliki batasan batasany terhadap akses informasi

w. Isolasi sistem yang sensitive

   Perlindungan sistem yang sensitif harus dijamin dan di atur oleh kebijakan yang berlaku

x. *Mobile computing* dan komunikasi

   Agar perusahaan membuat prosedur ini

y. Kerja jarak jauh

   Pengendalian kerja jarak jauh harus diatur dalam kebijakan yang formal.

Dalam dokumen SMKI tedapat kebijakan, prosedur, instruksi kerja dan sasaran terkait dengan pengembangan dan penerapan sistem keamanan informasi, adapun kebijakan yang harus dimiliki oleh perusahaan dari klausul keamanan fisik dan lingkungan, manajemen komunikasi dan operasi dan pengendalian akses adalah :

1. Kebijakan yang harus dipenuhi
   a. *Malicous Code Policy*
   b. *Access Control Policy*
   c. *Network Access Policy*
2. Prosedur yang harus dipenuhi
   a. *Physical Entry Control*

b. *Equipment Sy*
c. *Disposal of Info Equipment Device and Media*
d. *Loading and Unloading*
e. *Off-site Removal Authorisation*
f. *Documenting Operating Procedure*
g. *Change Control Procedure*
h. *Separation of Operational, Test and Development Environment Managing Third Parties*
i. *System Planning and Acceptance*
j. *Malicious Code Procedure*
k. *Back-up*
l. *Network Management*
m. *Media Handling*
n. *Business Information System*
o. *Monitoring*
p. *E-Commerce*
q. *User Access Rights*
r. *User Registration*
s. *Teleworker Procedure*
t. *Mobile Computing*
u. *Access Control Procedure*
v. *Secure Log-on*
w. *System Utilities*

3. Instruksi kerja yang harus dipenuhi
   a. *Fire Door*
   b. *Fire Alarms*
   c. *Burglar Alarms*
   d. *Fire Suppression Equipment*
   e. *Air Conditioning*

f. *Physical Perimeter Security Checklist*
g. *Netbook Configuration*
h. *Anti Malware*
i. *User Name Admin*
j. *Website Terms*
k. *Privacy Statement*
l. *Administrator Logging*
m. *Monitoring Schedule*
n. *Audit Logging Schedule*
o. *Teleworker User Agreement*
p. *User Agreement*
q. *Mobile Phone User*
r. *Wireless Notebook User*

4. Menyesuaikan sasaran dari seluruh pengendalian yaitu memastikan keamanan seluruh lokasi dan peralatan yang terdapat pada unit IT dan memastikan manajemen komunikasi dan operasi yang terdapat pada unit IT baik kepada pihak ketiga yang menyediakan jasa layanan terhadap sistem informasi serta pengendalian hak akses terhadap sistem informasi yang dilakukan oleh pengguna atau pegawai PT.KAI sudah dilakukan dan diterapkan dengan benar sesuai dengan yang dibutuhkan.