BAB IV SIMPULAN DAN SARAN

4.1 Simpulan

Simpulan yang dapat diambil dari hasil analisis dari klausul akuisisi pengembangan dan pemeliharaan sistem informasi, manajemen insiden keamanan, manajemen keberlanjutan bisnis, kesesuaian/kepatuhan adalah sebagai berikut:

1. PT.KAI sudah memastikan persyaratan keamanan dari sistem informasi. Namun dalam proses pengolahan aplikasi masih dinilai kurang baik, dimana kurangnya sosialiasi ke seluruh manajemen, sehingga memungkinkan terjadi modifikasi atau penyalahgunaan informasi dalam aplikasi. Kebijakan tentang penggunaan pengendalian kriptografi dinilai masih belum baik, namun dalam pengendalian manajemen kunci dinilai masih belum baik, dimana belum adanya aturan atau kebijakan yang mengatur. Pengendalian dan perlindungan dari keamanan *systems file* dinilai belum baik dimana belum semua dibuatnya instruksi kerja ataupun prosedur di seluruh jajaran manajemen. Penerapan perubahan pada aplikasi dinilai sudah baik oleh PT.KAI dimana sudah ada prosedur yang jelas, namun dalam mencegah peluang kebocoran informasi masih dinilai kurang baik dimana belum adanya sanksi yang jelas yang diberlakukan oleh PT.KAI apabila terjadi kebocoran informasi yang diakibatkan oleh pihak internal perusahaan.
2. Proses pelaporan kejadian terkait keamanan informasi sudah berjalan tetapi dari segi penerapannya dinilai masih kurang baik, dimana kurangnya koordinasi dari pihak manajemen dan juga disebabkan karena kurangnya kepedulian terhadap keamanan informasi. Tanggung jawab manajemen dan prosedur terkait insiden keamanan informasi serta perbaikannya sudah dijalankan, namun dalam penerapannya dinilai masih kurang baik oleh PT.KAI, dikarenakan kurangnya kegiatan

pemantauan dari setiap penanggung jawab dari masing-masing manajemen.

3. PT.KAI sudah memasukkan keamanan informasi dalam proses manajemen keberlanjutan bisnis, tetapi prosedur dalam pengembangan dan penerapannya masih belum ada dikarenakan masih dalam tahap perencanaan. Pemeliharaan tentang persyaratan informasi masih dalam tahap dimana pada waktu-waktu tertentu baru dijalankan, tetapi tidak mempunyai rencana yang berkelanjutan. Rencana bisnis masih belum diuji sehingga dinilai masih belum efektif secara keseluruhan oleh PT.KAI.
4. Peraturan perundang-undangan dan hukum masih dinilai belum diidentifikasi secara keseluruhan serta kebijakan mengenai hak paten penggunaan perangkat lunak masih belum lengkap dimana belum semua dipastikan kesesuaiannya dengan peraturan perundang-undangan maupun kontrak tentang penggunaan produk perangkat lunak yang digunakan. Pembatasan dalam penggunaan fasilitas pengolahan informasi dinilai belum berjalan dengan efektif oleh PT.KAI dikarenakan tidak berjalannya aturan yang berlaku. Kegiatan audit terhadap keamanan dinilai sudah baik oleh PT.KAI dimana sudah jelasnya tanggung jawab dan didokumentasikan secara formal.

4.2 Saran dan Rekomendasi

Saran yang dapat diambil dari kesimpulan berdasarkan klausul akuisisi pengembangan dan pemeliharaan sistem informasi, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis dan kesesuaian adalah sebagai berikut:

1. Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi
    a. Analisis Kebutuhan Keamanan dan Spesifikasi

Peningkatan terhadap sistem informasi yang ada harus menetapkan persyaratan untuk pengendalian manajemen pada PT.KAI.

b. Validasi Data Masukan

Data yang di masukkan kedalam aplikasi harus divalidasi untuk memastikan bahwa data tersebut benar dan tepat serta melakukan pemantauan secara regular untuk mencegah penyalahgunaan informasi.

c. Pengolahan Pengendalian Internal

Pengecekan validasi harus digabungkan ke dalam aplikasi untuk mendeteksi setiap kerusakan informasi karena kesalahan pengolahan atau tindakan yang disengaja, serta melakukan pengecekan ke setiap sistem informasi yang digunakan oleh PT.KAI.

d. Integritas Pesan

Setiap data yang dikelola dalam aplikasi harus diidentifikasi untuk memastikan bahwa data tersebut adalah benar.

e. Validasi Data Keluaran

Unit TI pada PT.KAI harus mengolah dan menyimpan setiap hasil pengolahan data dari aplikasi dengan benar dan tepat.

f. Kebijakan tentang Penggunaan Pengendalian Kriptografi

Membuat kebijakan tentang penggunaan pengendalian kriptografi dan harus dikembangkan untuk melindungi informasi PT.KAI.

g. Manajemen Kunci

Membuat prosedur yang mengatur mengenai pengendalian manajemen kunci dalam mendukung teknik kriptografi.

h. Pengendalian Perangkat Lunak yang Operasional

PT.KAI harus membuat prosedur untuk mengendalikan instalasi perangkat lunak pada sistem yang operasional.

i. Perlindungan Data Uji Sistem

PT.KAI harus membuat instruksi kerja yang formal dalam melakukan pengujian data serta data uji harus dipilih dan dilindungi serta dikendalikan.

j. Pengendalian Akses terhadap Kode Sumber Program

PT.KAI harus membuat instruksi kerja yang jelas untuk membatasi akses ke kode sumber program.

k. Prosedur Pengendalian Perubahan

Penerapan harus dikendalikan dengan menggunakan prosedur pengendalian yang formal.

l. *Review* Aplikasi setelah Perubahan Sistem Informasi

PT.KAI harus membuat prosedur untuk mengatur proses peninjauan dan pengujian terhadap sistem operasi yang diubah.

m. Perubahan Pembatasan pada Paket Perangkat Lunak

Unit TI pada PT.KAI harus melakukan pembatasan terhadap perubahan perangkat lunak dan hanya berfokus pada perubahan yang diperlukan saja untuk mengurangi dampak yang dapat merugikan organisasi.

n. Kebocoran Informasi

PT.KAI harus membuat aturan serta sanksi yang jelas (pidana atau perdata) agar meminimalisasi kebocoran informasi yang diakibatkan oleh pihak internal perusahaan.

o. Pengembangan Perangkat Lunak yang Dialihdayakan

Pengembangan perangkat lunak yang dialihdayakan harus disupervisi dan dipantau oleh organisasi.

p. Pengendalian Kerawanan Teknis

Informasi tepat waktu tentang kerawanan teknis dari sistem informasi yang digunakan harus diperoleh dan diambil tindakan untuk menangani resiko terkait.

2. Manajemen Insiden Keamanan Informasi
    a. Pelaporan Insiden Keamanan Informasi

       Unit TI pada PT.KAI harus mengkomunikasikan setiap kejadian dan kelemahan mengenai sistem informasi melalui manajemen terkait agar dilakukan tindakan koreksi secara tepat waktu.
    b. Pelaporan Kelemahan Keamanan

       Semua pegawai, kontraktor dan pihak ketiga dari sistem informasi dan layanan harus diisyaratkan oleh unit TI PT.KAI untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati dan dicurigai dalam sistem atau layanan.
    c. Tanggungjawab dan Prosedur

       Unit TI pada PT.KAI harus melakukan pemantauan bahwa setiap penanggung jawab dari masing-masing manajemen sudah melakukan tanggung jawabnya sesuai dengan prosedur yang berlaku.
    d. Pembelajaran dari Insiden Keamanan Informasi

       Unit TI pada PT.KAI harus membuat prosedur dalam mengatur mengenai pembelajaran mengenai insiden keamanan informasi.
    e. Pengumpulan Bukti

       Unit TI pada PT.KAI harus membuat *record* dalam proses pengumpulan bukti-bukti.
3. Manajemen Keberlanjutan Bisnis
    a. Memasukkan Keamanan Informasi dalam Proses Manajemen Keberlanjutan Bisnis.

       Setiap proses yang dikelola harus dikembangkan dan dipelihara oleh Unit TI pada PT.KAI untuk kebelanjutan bisnis organisasi

secara menyeluruh, yang menekankan penggunaan persyaratan keamanan informasi yang dibutuhkan untuk keberlanjutan bisnis.

b. Keberlanjutan Bisnis dan Manajemen Resiko

Unit TI pada PT.KAI harus mengidentifikasi setiap kejadian yang dapat menyebabkan gangguan terhadap proses bisnis organisasi, bersamaan dengan kemungkinan dan dampak dari gangguan tersebut serta konsekuensinya terhadap keamanan informasi.

c. Mengembangkan dan Menerapkan Rencana Keberlanjutan termasuk Keamanan Informasi.

Unit TI pada PT.Kai harus membuat prosedur mengenai pengendalian manajemen keberlanjutan bisnis dan harus dikembangkan untuk memelihara dan memastikan ketersediaan informasi pada tingkat dan dalam jangka waktu yang diisyaratkan setelah terjadinya gangguan dari proses bisnis.

d. Kerangka Kerja Perencanaan Keberlanjutan Bisnis

Unit TI pada PT.KAI harus membuat kerangka kerja yang jelas dari perencanaan yang keberlanjutan dalam memelihara dan memastikan semua rencana secara konsisten.

e. Pengujian, Pemeliharaan dan *Assessment* Ulang Rencana Keberlanjutan Bisnis.

Unit TI pada PT.KAI harus memastikan secara efektif bahwa rencana keberlanjutan bisnis harus diuji dan dimuktahirkan secara regular.

4. Kesesuaian/Kepatuhan

a. Identifikasi Peraturan Hukum yang Berlaku

Unit TI pada PT.KAI harus mengidentifikasi setiap peraturan dan perundang-undangan dan kewajiban kontrak dalam menjaga keamanan dari sistem informasi dan organisasi.

b. Hak Kekayaan Intelektual

Unit TI pada PT.KAI harus membuat kebijakan mengenai hak kekayaan intelektual yang secara jelas diidentifikasi aturan perundang-undangan dan kontrak mengenai perangkat lunak yang dipakai oleh organisasi.

c. Perlindungan Rekaman Organisasi

   Unit TI pada PT.KAI harus melakukan pemantauan terhadap setiap rekaman terkait kegiatan yang berlangsung untuk meminimalisasi terjadinya kehilangan data ataupun informasi dari organisasi.

d. Perlindungan Data dan Rahasia Informasi Pribadi

   Unit TI pada PT.KAI harus membuat sebuah regulasi atau aturan yang mengatur tentang perlindungan data dan informasi dari organisasi secara jelas yang dipersyaratkan dalam legislasi, regulasi yang relevan, dan klausul kontrak jika diperlukan.

e. Pencegahan Penyalahgunaan Fasilitas Pengolahan Informasi

   Unit TI pada PT.KAI harus melakukan pemantauan terhadap kegiatan penggunaan fasilitas pengolahan informasi untuk mencegah terjadinya penggunaan fasilitas pengolahan informasi dengan tujuan yang tidak sah.

f. Regulasi Pengendalian Kriptografi

   Unit TI pada PT.KAI harus membuat regulasi mengenai pengendalian kriptografi yang sesuai dengan aturan dan perundang-undangan.

g. Pemenuhan Terhadap Kebijakan Keamanan dan Standar

   Unit TI pada PT.KAI harus membuat instruksi kerja dimana tanggung jawab dari setiap manajer secara jelas diidentifikasi dalam proses pemenuhan kebijakan keamanan informasi.

h. Pengecekan Pemenuhan Teknis.

Unit TI pada PT.KAI harus mengecek setiap sistem informasi yang dipakai secara regular dan dicek pemenuhan teknis terhadap standar penerapan keamanan.

i. Pengendalian Audit Sistem Informasi

Unit TI pada PT.KAI harus melakukan pengecekan yang dilakukan oleh bagian audit TI terhadap sistem informasi yang dipakai yang sudah direncanakan dan sudah disetujui oleh pihak manajemen terkait.

j. Perlindungan terhadap Alat Audit Informasi

Unit TI pada PT.KAI harus membuat prosedur mengenai perlindungan terhadap alat audit sistem informasi dimana akses terhadap pemakaian alat audit harus dibatasi dan dilindungi.

Penekanan dan penyesuaian dari klausul-klausul pada pokok masalah yang diambil yaitu pengembangan akuisisi sistem informasi dan pemeliharaan, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis, kepatuhan/kesesuaian harus dipenuhi. Berikut adalah rekomendasi dari hasil analisis pada BAB III, referensi penulisan dokumen ISO 27001:2005 dapat dilihat pada lampiran C (*Policy*), D (*Procedure*), E (*Work Instruction*), F (*Record*).

1. Dalam pembuatan dokumen SMKI harus memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran, dan rencana terkait dengan pengembangan, penerapan, dan peningkatan SMKI. Adapun dokumen kebijakan yang harus dipenuhi dari klausul pengembangan akuisisi sistem informasi dan pemeliharaan, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis, kepatuhan/kesesuaian adalah sebagai berikut:
    a. *Intellectual Property Rights.*
    b. *Data Protection and Privacy.*

2. Dalam pembuatan prosedur dan panduan yang sedang dikembangkan oleh PT.KAI, harus memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Berikut adalah prosedur yang harus dipenuhi dari klausul pengembangan akuisisi sistem informasi dan pemeliharaan, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis, kepatuhan/kesesuaian:
    a. *Cryptographic Key Management.*
    b. *Control of Operationanl Software.*
    c. *Vulnerability management.*
    d. *Reporting Information Securiry Weaknesses and Events.*
    e. *Responding to Information Security Reports.*
    f. Collection of Evidence.
    g. *Business Continuity Planning.*
    h. Business Continuity Plan
    i. Business Continuity Risk Assessments
    j. Testing, Maintaining and Reassessing BC Plans.
3. Pembuatan dokumen petunjuk teknis atau instruksi kerja yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ketingkatan teknis. Adapun dokumen instruksi kerja yang harus dipenuhi dari klausul pengembangan akuisisi sistem informasi dan pemeliharaan, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis, kepatuhan/kesesuaian sebagai berikut:
    a. Schedule of Required Cryptographic Controls.
    b. IPR Compliance Procedure
    c. *Retention of Records.*
    d. *Compliance and Compliance Checking Procedure.*
    e. Systems Auditing Procedure.
    f. Info.Security Weakness and Event Checklist

g. Schedule of Information Security Event Reports

4. Menyesuaikan sasaran pengendalian dalam proses yang dimaksud adalah akuisisi sistem informasi dan pemeliharaan, manajemen insiden keamanan informasi, manajemen keberlanjutan bisnis, kesesuaian/kepatuhan.

    a. Akuisisi Sistem Informasi dan Pemeliharaan

    Sasaran dalam proses ini adalah untuk memastikan bahwa keamanan merupakan bagian utuh dari sistem informasi dalam melindungi kerahasiaan, keaslian, integritas informasi, serta pengelolaan yang benar dalam perangkat lunak sistem aplikasi dan informasi dan juga mengurangi resiko terhadap kerawanan teknis yang dipublikasikan.

    b. Manajemen Insiden Keamanan Informasi

    Sasaran dalam proses ini adalah untuk memastikan kejadian dan kelemahan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu.

    c. Manajemen Keberlanjutan Bisnis

    Sasaran dalam proses ini adalah untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dan efek kegagalan utama sistem informasi dan untuk memastikan keberlanjutan secara tepat waktu.

    d. Kesesuian/Kepatuhan

    Sasaran dalam proses ini adalah untuk mencegah pelanggaran terhadap undang-undang peraturan atau kewajiban dan persyaratan keamanan.