Audit Keamanan Sistem Informasi IT Di PT X

Fandy Arya Gunadi[1], Adi Wibowo[2], Ibnu Gunawan[3]
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031) – 2983455 - Fax. (031) - 8417658
E-mail: fandy534@yahoo.com[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK

Berdiri pada tanggal 10 Juli 1991 di Sidoarjo, Jawa Timur, PT X adalah perusahaan yang bergerak di bidang percetakan umum, terutama mencetak dokumen niaga. Dalam menjalankan proses bisnisnya, perusahaan ini menggunakan *software, hardware*, jaringan, dan mesin yang digunakan untuk proses produksi. Tetapi perusahaan merasa kurang memperhatikan masalah*security* akan aset dan data yang dimiliki perusahaan. Padahal *data* dan informasi sekarang ini sudah menjadi aset yang sangat penting. Maka dari itu dibutuhkan audit sistem informasi yang bertujuan untuk menganalisis sejauh mana sejauh mana tingkat keamanan sistem informasi perusahaan.

Pada skripsi ini dilakukan analisa audit sistem informasi terhadap keamanan ITyang ada di PT. X. Langkah-langkah dalam melakukan analisa audit tersebut yaitu dengan menggunakan standar COBIT 4.1 .Masalah-masalah yang ditemukan di perusahaan dari antara lain tidak ada surat tugas yang diberikan kepada karyawan IT di PT X, tidak ada laporan bulanan tentang keamanan IT yang dibuat oleh divisi IT PT X, tidak ada standar keamanan IT yang menjadi acuan di perusahaan, tidak menggunakan kunci kriptografi yang diterapkan di dalam melindungi data dan informasi.

Respon yang diberikan kepada perusahaan yaitu sebaiknya perusahaan membuat surat tugas dan membuat laporan bulanan tentang keamanan IT. Segera juga untuk membuat standar keamanan IT dan membuat kunci kriptografi untuk melindungi dan dan informasi yang dimiliki oleh peruhahaan.

Dalam penelitian ini membahas 1 domain yaitu *Deliver and Support* dari 4 domain yang ada di COBIT dengan pembahasan dibatasi pada *ensure system security*(DS5).

Kata Kunci: Audit Sistem Informasi Keamanan IT, COBIT 4.1, metode kualitatif.

ABSTRACT

Established on July 10, 1991 in Sidoarjo, East Java, PT X is a company engaged in the field of general printing, especially printing commercial documents. In carrying out its business processes, the company is using software, hardware, network, and machines used for the production process. But the company was less concerned about security for asset and data owned companies. Though the data and information are now becoming a very important asset. Thus the required audit information system that aims to analyze the extent to which extent the company's information system security.

This thesis analyzed informationsystem security audit of IT in PT. X. The steps in the audit analysis is by using COBIT 4.1 standards. Problems were found in the company of, among others, there is no assignment letter given to employees of IT in PT X, no monthly report on IT security made by the IT division of PT X, there is no IT security standards as the reference in the company, not using cryptographic key features implemented in protecting data and information.

The response given to the company that the company should make a task and make monthly reports on IT security. Soon also to make IT security standards and create cryptographic keys for protecting and and information held by company.

In this study discusses one domain that Deliver and Support of 4 domain in COBIT the discussion is limited to Ensure systems security (DS5).

Keywords: *Audit Information System*, COBIT 4.1, *qualitative methods.*

1. PENDAHULUAN

Di jaman era globalisasi saat ini teknologi sangatlah berkembang dengan pesat. Begitu juga dengan perkembangan teknologi dan sistem informasi pada perusahaan semakin pesat, resiko keamanan yang melekat pada informasi perusahaan juga semakin besar. Lemahnya kendali keamanan atas aset informasi memudahkan pihak-pihak yang tidak bertanggung jawab untuk mencuri informasi atau menganggu jalannya proses produksi perusahaan tersebut. Untuk itu perusahaan sangat membutuhkan perlindungan keamanan aset karena aset merupakan bagian yang penting bagi kelangsungan proses bisnis pada perusahaan.

PT X adalah sebuah perusahaan yang bergerak di bidang percetakan. Data dan informasi sudah menjadi aset penting dalam perusahaan. Untuk mengantisipasi hal-hal yang tidak diinginkan berkaitan dengan penyalahgunaan data dan informasi maka perlu dilakukan audit. Kebijakan tentang keamanan sistem merupakan salah satu aspek yang sangat penting dalam sebuah sistem informasi. Audit Sistem Informasi menjadi sebuah solusi untuk mengukur sejauh mana tingkat keamanan Sistem Informasinya. Untuk melaksanakan Audit Sistem Informasi, perlu memiliki standar yang baik untuk dapat dibandingkan dengan standar milik perusahaan. Kerangka kerja *Control Objective for Information dan Related Technology* (COBIT)mempunyai tujuan untuk mengendalikan TI terkait dan merupakan suatu standar yang telah diakui cukup baik pada tingkat internasional. Dalam analisa ini dibahas 1 Domain yang ada di dalamCOBIT yaitu *Deliver and Support* dari 4 domain yang ada di COBIT dengan pembahasan dibatasi pada tingkat *Ensure System Security(DS 5).*

Pada setiap perusahaan yang memiliki aset-aset yang penting, keamanan atas aset-aset tersebut merupakan salah satu hal yang penting untuk dilakukan. Dengan adanya audit sistem keamanan informasi pada sistem PT X dapat meningkatkan keamanan informasi dan menurunkan risiko keamanan informasi.

2. LANDASAN TEORI

2.1 Pengertian Audit Sistem Informasi

Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari

suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan.[2]
Audit SI sebagai proses pengumpulan dan evaluasi bukti-bukti untukmenentukan apakah sistem informasi dapat melindungi aset, teknologi yang adatelah memelihara integritas *data* sehingga keduanya dapat diarahkan kepadapencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efisien.[1]
Control Objectives for Information and Related Technology (COBIT)diperkenalkan pada tahun 1996 oleh *The Information System Audit and ControlAssosiation*. Pada tahun 1998 *IT Governance Institute* (ITGI) berdiri dengantujuan untuk memimpin riset pada area vital tata kelola teknologi informasi. Padatahun yang sama *The Information System Audit and Control Assosiation* dan ITGImelebur menjadi satu entitas dan mempublikasikan COBIT edisi ketiga padatahun2000 dan diikuti versi keempat pada tahun 2006.[3]
COBIT dikelompokkan kedalam 4 *domain*, yaitu :

1. Plan and Organize (PO)

Domain ini mencakup strategi, taktik dan perhatian pada identifikasi carateknologi informasi dapat berkontribusi terbaik pada pencapaian objektifbisnis. Selanjutnya, realisasi visi strategis perlu direncanakan, dikomunikasikandan dikelola untuk perspektif yang berbeda. Akhirnya suatu organisasi yangtepat seperti halnya infrastruktur teknologi harus diletakkan pada tempatnya.

2. Acquired and Implement (AI)

Guna merealisasikan strategi teknologi informasi, solusi teknologi informasi perludiidentifikasi, dikembangkan atau diperoleh seperti halnya diimplementasikan dandiintegrasikan kedalam proses bisnis. Sebagai tambahan, perubahan dalampemeliharaan sistem yang ada dicakup dalam domain ini untuk memastikan solusiberlangsung untuk memenuhi objektif bisnis.

3. Deliver and Support (DS)

Domain ini dihubungkan dengan penyampaian sesungguhnya layanan yangdiperlukan. Mencakup penyediaan layanan, manajemen keamanan dankelangsungan, dukungan layanan pada pengguna, manajemen data dan fasilitasoperasional.

4. Monitor and Evaluate (ME)

Semua proses teknologi informasi perlu secara rutin dinilai dari waktu kewaktu untuk kualitas dan pemenuhan dengan kebutuhan kontrol. Domain iniberkenaan dengan manajemen kinerja, pemantauan kontrol internal,pemenuhan terkait dengan regulasi dan pelaksanaan tata kelola.

2.2 Metode Audit Sistem Informasi

Dalam melaksanakan audit Sistem Informasi diterapkan metodologi audit Sistem Informasi yang sesuai dengan metodologi yang diajukan oleh *IT Assurance Guide: Using* COBIT. Pada dasarnya dalam metodologi audit, dilakukan metodologi pengumpulan *data*, yang meliputi Observasi dan wawancara dilakukan dengan pihak terkait.[4]

Tahapan audit tersebut adalah:

1. Penentuan *audit resources*
Tahap ini bertujuan mengumpulkan seluruh dokumen yang diperlukan untuk proses audit, meliputi :

- Seluruh *Standard Operating Procedure* (SOP) divisi IT PT X.
- Laporan keamanan bulanan divisi IT PT X.
- Laporan bulanan *programmer*.

Selain mengumpulkan dokumen, tahap ini juga menghubungi orang-orang yang berhubungan dengan pengadaan dan perawatan aplikasi di lingkup perusahaan untuk meminta kesediaan mengisi kuesioner, melakukan *interview*, dan melakukan pertemuan penyamaan pendapat. [5]

2. Evaluasi Kontrol
Tahap ini bertujuan mengetahui apakah seluruh kontrol yang telah diterapkan pada perusahaan dapat memenuhi standar yang diberikan oleh COBIT 4.1. Kontrol yang dimaksud adalah seluruh peraturan, standar prosedur, dan struktur organisasi (baik jabatan, atau divisi) yang bertanggung jawab terhadap proses pengadaan dan perawatan aplikasi.

Tahap ini sangat penting dilakukan karena bila kontrol yang sudah ada dapat secara efektif memenuhi standar COBIT tersebut, berarti kontrol dapat digunakan sebagai standar untuk pengukuran berikutnya, yaitu *Compliance Test*. Tetapi bila berdasarkan evaluasi kontrol, kontrol itu sendiri tidak memadai untuk menjadi standar pengujian, maka proses pengukuran berikutnya tidak menggunakan kontrol, tetapi evaluasi substansi proses signifikan.

Untuk mengukur kontrol berdasarkan kriteria, maka diputuskan skala yang diperlukanuntuk mengukur pemenuhan setiap kriteria kontrol, yaitu:

- Tidak efektif
  Tidak ada kontrol yang tercatat, atau yang dilakukan walau tidak tercatat, yang memenuhi kriteria yang dimaksud.
- Efektif dengan perbaikan besar
  Kontrol hanya memenuhi sebagian kecil kriteria. Prosedur yang telah dilakukan walaupun tidak tercatat dalam kebijakan / peraturan belum dapat memenuhi kriteria lainnya tersebut.
- Efektif dengan perbaikan kecil
  Kontrol telah memenuhi sebagian besar kriteria, tetapi terdapat beberapa prosedur yang telah dilakukan walaupun tidak tercatat dalam kebijakan / peraturan yang dapat memenuhi kriteria lainnya tersebut
- Efektif
  Seluruh kontrol telah memenuhi kriteria yang disebutkan.

3. Evaluasi Kesesuaian Proses terhadap Kontrol (*Compliance Test*)
Tahap ini dilakukan bila kontrol dinyatakan dapat secara efektif mencapai gambaran ideal proses yang dinyatakan oleh COBIT 4.1. Tahap ini membandingkan antara proses sesungguhnya yang terjadi di lapangan dengan kontrol (peraturan, dan standar prosedur) untuk memeriksa apakah proses sesungguhnya tersebut telah dilaksanakan dengan konsisten. Juga dilakukan evaluasi apakah telah terdapat upaya monitoring yang memadai untuk melakukan evaluasi berkala proses terhadap kontrol.

Untuk standar penilaian evaluasi proses untuk *Control Practices* yang dipakai adalah *control Practices* yang sama dengan evaluasi kontrol, tetapi menggunakan standar penilaian yang berbeda. Perbedaan standar penilaian disesuaikan dengan tujuan evaluasi, yaitu mencari tahu apakah terdapat jaminan bahwa proses yang dijalankan oleh PT X selama ini akan mencapai *control Practices*, atau tidak.

Standar penilaian evaluasi proses adalah:

- *Assurance*
  Proses dijamin memenuhi *control Practices* bila dilakukan dengan konsisten seperti waktu pelaksanaan audit.
- *Assurance with Modification*
  Proses masih bisa dijamin dapat memenuhi *control Practices* bila dilakukan perubahan pada proses tersebut.
- Non Assurance
  Proses tidak dijamin memenuhi *control Practices* karena pada saat dilakukan audit, proses tidak mampu menunjukkan kinerja yang menuju pencapaian *control Practices* tersebut. Proses yang mendapatkan penilaian ini perlu diberi penyesuaian seperti yang dijelaskan pada setiap bagian proses evaluasi.

4. Evaluasi Substansi Terbatas (*Limited Substantive Test*)
   Tahap ini dilakukan setelah tahap ketiga. Walaupun pada tahap ketiga biasanya sudah dapat diketahui apakah sebuah proses dijamin (*assured*) dapat mencapai target proses tersebut bila sesuai (*comply*) terhadap kontrol, tetapi dapat terjadi bahwa kesimpulan tidak dapat diambil dengan absolut. Untuk mengatasi masalah ini maka proses-proses yang tidak dapat dievaluasi secara absolut memerlukan uji substansi dengan memanfaatkan dokumen-dokumen proses, kuesioner, dan *interview* terhadap pelaku proses agar dapat mengambil keputusan. Jadi tahap ini tidak dilakukan untuk seluruh aspek audit, melainkan hanya untuk proses-proses yang memerlukan pengujian lebih lanjut.
5. Evaluasi Substansi Signifikan (*SignificantSubstantiveTest*)
   Tahap ini dilakukan bila tahap kedua menunjukkan bahwa kontrol itu sendiri tidak dapat secara efektif mencapai gambaran ideal dari control objectives. Tahap ini dilakukan dengan metode yang sama seperti tahap keempat. Yang menjadi perbedaan adalah cakupan aspek yang diuji adalah semua aspek pengadaan dan perawatan aplikasi tanpa melihat apakah kontrol untuk aspek tersebut efektif atau tidak.
6. Pengukuran *Maturity Level*.
   Pengukuran *maturity level* adalah tahapan yang bertujuan memberikan informasi *level* perbandingan antara kondisi aktual dalam perputakaan, dengan kondisi ideal yang dimiliki oleh industri. Kondisi ideal selalu dinyatakan pada *level* 5. Dengan membandingkan *level* ini diharapkan memberi informasi aspek-aspek perbaikan yang perlu dilaksanakan untuk meningkatkan *level* tersebut.
7. Penentuan kesimpulan dan rekomendasi
   Dengan memperhatikan hasil dari tahap kedua hingga keenam. Rekomendasi dibuat selain berdasarkan hasil evaluasi *control objectives*, juga memanfaatkan pengalaman dan *judgement profesional* dari auditor.[6]

3. MODEL DAN STRATEGI BISNIS

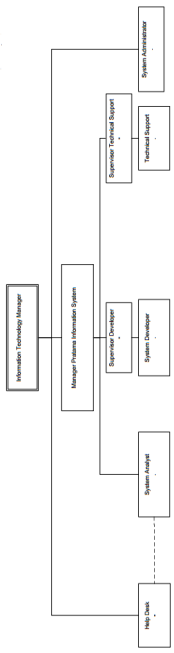
3.1 Perusahaan Percetakan PT X

PT X Berdiri pada tanggal 10 Juli 1991 di Sidoarjo, Jawa Timur. Pada awalnya perusahaan hanya bergerak di bidang percetakan umum, terutama mencetak dokumen niaga. Pada tahun 1996 PT X menerima lisensi dari BOTASUPAL untuk mencetak dokumen sekuriti. Pada saat ini PT X telah maju berkembang dan memiliki tiga pabrik utama, yaitu pabrik untuk mencetak dokumen sekuriti, pabrik untuk memproduksi kartu VISA & Master dan kartu sekuriti lainnya, serta pabrik untuk mencetak dokumen niaga. Ketiganya dibangun secara modern dan berada dalam lingkungan yang tertata asri serta dilengkapi dengan sistem dan peralatan terkini untuk menunjang kelancaran dan kinerja perusahaan untuk memberikan hasil yang maksimal.

Model Bisnis perusahaan adalah job order, proses bisnis yang dilakukan apabila ada order yang kita terima dari konsumen. Setiap detail pekerjaan 100% ditentukan oleh calon pembeli, pihak pembuat hanya menyatakan kesanggupannya. Bila pekerjaan telah disetujui, maka dilakukan negosiasi harga antara pembeli dan pembuat. Dalam proses negosiasi tersebut tentunya masing-masing pihak telah mengetahui prakiraan harga barang atau jasa yang ingin dikerjakan tsb. Pastinya untuk urusan yang satu tersebut membutuhkan waktu yg panjang hanya untuk negosiasi kecocokan harga.

3.2 Struktur Organisasi Divisi IT PT X.

Ini adalah detail Struktur organisasi yang ada di PT X.



Gambar 3.2 Struktur Organisasi Divisi IT PT X

Tugas dan wewenang Divisi IT yang dijalankan pada PT X sebagai berikut:

- Melakukan inventaris aset-aset IT.
- Menerima komplain dan mendistribusikan ke *Engineer*.
- Melakukan aktifitas korespondensi
- Membuat laporan analisa sasaran mutu.
- Membuat laporan analisa komplain per minggu.
- Membuat notulen dari setiap meeting.
- Membuat Permintaan Pembelian Barang(PPB).
- Memberikan solusi pada komplain-komplain yang bersifat *generic* (sudah ada pada *Knowledge base*).
- Melakukan pemeliharaan sistem informasi JDE yang sudah ada agar dapat beroperasi sebagaimana mestinya.

- Mengembangkan sistem informasi JDE sesuai perkembangan proses bisnis yang sudah ditetapkan oleh manajemen perusahaan.
- Mengolah data transaksional dari ERP menjadi data analisis yang bisa digunakan bagi eksekutif sebagai dasar dalam pengambilan keputusan.
- Membuat program untuk *numbering* atau personalisasi dengan Delphi, Scitex atau Nipson.
- Membuat aplikasi berbasis *smartcard* yang dilengkapi fitur *fingerprint*, atau *face recognition.*
- Membuat aplikasi personalisasi percetakan *cheque*/bilyet giro.
- Membuat aplikasi sistem informasi internal baik JDE maupun non JDE seperti *payroll*.
- Memberikan support kepada departemen lain yang berhubungan dengan solusi-solusi IT.
- Memberikan support kepada departemen *Marketing* untuk solusi IT yang dapat memberikan nilai tambah terhadap dokumen-dokumen yang dihasilkan perusahaan.
- Melakukan *Research and Development* tentang teknologi baru di IT yang bisa mendukung dan memberi nilai tambah terhadap produk-produk perusahaan.
- Memelihara komputer *Workstation* dan *Hardware* pendukung yang digunakan dalam operasional perusahaan.
- Melakukan *monitoring* terhadap penerapan IT *Policy* yang sudah ditetapkan.
- Mengusulkan infrastruktur IT yang efisien dan pengimplementasian teknologi IT tepat guna untuk mendukung kebutuhan perusahaan dan departemen IT. Misal: *Source Control, File Server, Document Management, IT Asset Management, Project Management* dan *Issue Tracking.*
- Memelihara dan memberikan support terhadap mesin-mesin produksi yang dikendalikan oleh sistem komputer seperti: *Scitex, Nipson, Printonix* dan *Laser Perforator.*
- Menjamin semua perangkat IT terutama yang berhubungan dengan *server*, dan *network* agar berfungsi dengan optimal yang dilengkapi dengan instruksi kerja yang detail.
- Membuat perencanaan yang berhubungan dengan BCP (*Business Plant Continuity*) dan DRP (*Disaster Recovey Planning*) misal: *Sistem Backup* dan *Restore, Fail Over Sistem* dsb sesuai kebutuhan perusahaan.
- Melakukan administrasi terhadap jaringan komputer di dalam perusahaan seperti: hak akses dan manajemen penyimpanan *file*, E-Mail, akses internet, Pengaturan Bandwitdh, dll.
- Melakukan *monitoring* terhadap segala aktifitas di jaringan yang mencurigakan seperti *Virus, Worm , Malware, Spam, Hacker, Intrusion detection, Invalid Entry, CCTV*, dll.
- Melakukan monitoring terhadap penerapan IT *Policy* yang sudah ditetapkan.

4. ANALISA AUDIT & PEMBAHASAN

4.1 Pembentukan Kriteria Evaluasi Kontrol

Berdasarkan pertimbangan-pertimbangan kriteria lengkap untuk mengevaluasi control

yang sudah ada adalah:

1. *DS 5.1 Management of IT Security*
    a. Periksa Surat Tugas untuk divisi IT *security*
    b. Periksa Surat pengangkatan/dokumen/notulen rapat penunjukan *charter*
    c. Periksa Surat pengangkatan/dokumen/notulen rapat struktur organisasi IT *security*.
    d. Periksa Laporan dari IT *security*.

2. *DS 5.2 IT Security Plan*
    a. Periksa apakah IT *security* PT X mempertimbangkan:
        i. *Policy* dan Standar IT *security.*
        ii. SOP untuk melaksanakan dan menegakkan *policy* dan standar.
        iii. Dokumen/notulen rapat untuk peran dan tanggung jawab karyawan untuk menjaga informasi perusahaan.
        iv. Persyaratan *Staffing*.
        v. Jadwal *Security awareness* dan pelatihan rutin.
        vi. Dokumen/notulen rapat untuk praktek penegakan pelanggaran Standar Keamanan Perusahaan.
        vii. Investasi untuk keamanan informasi.
    b. Periksa Dokumen/notulen rapat kebutuhan/daftar kebutuhan keamanan dari:
        i. Rencana taktis IT.
        ii. Klasifikasi data.
        iii. Standar teknologi.
        iv. Kebijakan keamanan dan control.
        v. Manajemen resiko.
        vi. Persyaratan aturan pihak luar.
    c. Periksa Dokumen/notulen rapat yang membantu pembuatan kebutuhan IT *security*:
        i. Pengembangan SLA dan OLAs.
        ii. Otomatisasi persyaratan solusi.
        iii. Aplikasi perangkat lunak .
        iv. Komponen infrastruktur IT.
    d. Periksa Dokumen/notulen rapat sosialisasi prosedur dan kebijakan keamanan IT kepada *stakeholder* dan *user*.

3. *DS 5.3 Identity Management*
    a. Periksa SOP/dokumen/catatan/notulen rapat untuk IT *security* tentang:
        i. Identifikasi *user* secara unik.
        ii. Mekanisme otentikasi dan otorisasi.
        iii. Hak akses.
    b. Pastikan SOP/Dokumen/catatan/notulen rapat bahwa peran dan kriteria otorisasi akses untuk menetapkan hak akses pengguna memperhitungkan:
        i. Sensitifitas informasi dan aplikasi yang terlibat (klasifikasi data).
        ii. Kebijakan untuk perlindungan informasi dan diseminasi (hukum, peraturan, kebijakan internal dan persyaratan kontrak).
        iii. Peran dan tanggung jawab sebagaimana didefinisikan dalam perusahaan.
        iv. Hak akses perlu untuk dimiliki terkait dengan fungsi.
        v. Standard tetapi individu akses pengguna profil untuk peran pekerjaan umum dalam organisasi.
        vi. Persyaratan untuk menjamin pemisahan tugas yang tepat.
    c. Periksa metode untuk otentikasi dan otorisasi pengguna untuk menetapkan tanggung jawab dan menegakkan hak akses sesuai dengan sensitivitas informasi dan fungsional persyaratan aplikasi dan komponen infrastruktur, dan sesuai dengan hukum

yang berlaku, peraturan, kebijakan internal dan perjanjian kontrak.

d. Periksa SOP/dokumen/notulen rapat untuk:
   i. Identifikasi *user* baru.
   ii. *Recording*.
   iii. *Maintaining* dan *approving* hak akses.

e. Periksa SOP/dokumen/notulen rapat/catatan yang dilakukan perusahaan pada:
   i. Hak akses karyawan saat karyawan tersebut pindah pekerjaan.
   ii. Karyawan dipecat dan pindah jabatan.

4.2. Standar Penilaian Evaluasi Kontrol

Untuk mengukur kontrol berdasarkan kriteria, maka diputuskan skala yang diperlukanuntuk mengukur pemenuhan setiap kriteria kontrol, yaitu:

- Tidak efektif
  Tidak ada kontrol yang tercatat, atau yang dilakukan walau tidak tercatat, yang memenuhi kriteria yang dimaksud.
- Efektif dengan perbaikan besar
  Kontrol hanya memenuhi sebagian kecil kriteria. Prosedur yang telah dilakukan walaupun tidak tercatat dalam kebijakan / peraturan belum dapat memenuhi kriteria lainnya tersebut.
- Efektif dengan perbaikan kecil
  Kontrol telah memenuhi sebagian besar kriteria, tetapi terdapat beberapa prosedur yang telah dilakukan walaupun tidak tercatat dalam kebijakan / peraturan yang dapat memenuhi kriteria lainnya tersebut
- Efektif
  Seluruh kontrol telah memenuhi kriteria yang disebutkan.

4.3.Penilaian Evaluasi Kontrol

Evaluasi kontrol dilakukan dengan melakukanwawancara "Evaluasi Kontrol" yangdilakukan pada kepala IT dan karyawan IT di lingkup Divisi IT PT X. Berdasarkanjawaban dan pertimbangan dari kriteria evaluasi kontrol, maka hasil evaluasi kontrol yangsudah ada sebagai berikut:

1. *DS 5.1 Management of IT Security*: Efektif dengan perbaikan besar
   a. Tidak ada surat tugas, tugas untuk Divisi IT hanya diberikan secara aktual tidak dicatat.
   b. Memiliki dokumen tentang penunjukan charter.
   c. Tidak memiliki struktur organisasi untuk IT *Security*, hanya ada Struktur Organisasi untuk divisi IT.
   d. Tidak ada laporan rutin.

2. *DS 5.2 IT Security Plan* : Efektif dengan perbaikan besar
   a. Analisa kontrol untuk DS 5.2.a tentang pertimbangan divisi IT PT X :
      i. Belum ada peraturan (termasuk standar prosedur) untuk menentukan *Policy* dan Standar IT *Security*
      ii. Memiliki dokumen untuk melaksanakan dan menegakkan *policy* dan standar, contoh: kebijakan *USB Block*.
      iii. Belum ada peraturan dan dokumen untuk peran dan tanggung jawab karyawan untuk menjaga informasi perusahaan.
      iv. Tidak ada persyaratan *Staffing*.
      v. Tidak ada jadwal *security awareness* dan pelatihan rutin.
      vi. Tidak memiliki peraturan(termasuk standar prosedur) untuk praktek penegakan pelanggaran Standar Keamanan Perusahaan, bila terjadi pelanggaran pelaku hanya diberikan peringatan.
      vii. Investasi untuk keamanan IT cukup baik seperti pengadaan perangkat jaringan, pengadaan *server*, pemasangan CCTV dan *fingerprint*.
   b. Analisa kontrol untuk DS 5.2.b tentang kebutuhan keamanan PT X:
      i. Ada rencana taktis IT seperti pembuatan standar ISO 27001, mengundang konsultan.
      ii. Tidak ada klasifikasi data
      iii. Belum ada Standar Teknologi.
      iv. Memiliki kebijakan keamanan dan kontrol seperti menegakan *USB Block*, Otentifikasi *user*, Kebijakan *Email*.
      v. Belum ada manajemen resiko.
      vi. Memiliki persyaratan aturan untuk pihak luar.
   c. Analisa kontrol untuk DS 5.2.c tentang saran pembuatan kebutuhan IT Security:
      i. Belum ada dokumen untuk pengembangan SLA dan OLAs untuk IT *security plan*.
      ii. Belum ada dokumen untuk otomatisasi persyaratan solusi.
      iii. Belum ada dokumen untuk aplikasi perangkat lunak.
      iv. Komponen infrastruktur yang sudah ada cukup baik yaitu meliputi *CCTV*, *fingerprint*, perangkat jaringan, *server*.
   d. Memiliki dokumen sosialisasi prosedur dan kebijakan keamanan IT kepada *stakeholder* dan *user*.

3. *DS 5.3 Identity Management* : Efektif dengan perbaikan besar
   a. Analisa kontrol untuk DS 5.3.a tentang dokumen untuk:
      i. Mengidentifikasi *user* secara unik dengan mengunakan trax studio.
      ii. Tidak ada SOP atau dokumen untuk menentukan mekanisme otentifikasi dan otorisasi hanya dilaksanakan secara aktual tetapi tidak didokumentasikan.
      iii. Hak akses setiap user disimpan di dalam Trax studio.
   b. Analisa kontrol untuk DS 5.3.b tentang Pertimbangan peran dan kriteria otorisasi akses untuk menetapkan hak akses pengguna:
      i. Sensitifitas Informasi dan aplikasi yang terlibat diperhitungkan oleh PT X, tetapi tidak dicatat.
      ii. Tidak ada kebijakan untuk perlindungan informasi dan diseminasi, bila *user* melakukan pelanggaran hanya diberikan teguran.
      iii. Tidak ada dokumen atau catatan untuk pembagian hak akses sesuai peran dan tanggung jawab sebagaimana didefinisikan perusahaan hanya dilakukan secara aktual saja.
      iv. Hak akses diberikan sesuai dengan fungsi dan peran *user* tetapi tidak dicatat dan didokumentasikan.
      v. Tidak ada standar individual akses pengguna profil untuk peran pekerjaan umum dalam organisasi.

vi. Tidak ada prosedur persyaratan untuk pemisahan tugas yang tepat.

c. Tidak ada prosedur otorisasi dan otentifikasi untuk menetapkan tanggung jawab dan menegakkan hak akses sesuai dengan sensitivitas informasi dan fungsional persyaratan aplikasi dan komponen infrastruktur dan sesuai dengan hukum yang berlaku. Tetapi ada perjanjian kontrak hak akses selama 24 jam bila ada permintaan dari divisi yang terkait kepada divisi IT PT X.

d. Analisa kontrol untuk DS 5.3.d:
   i. Tidak ada prosedur atau dokumen identifikasi *user* baru hanya dilakukan secara aktual dalam aplikasi.
   ii. Tidak ada prosedur atau dokumen untuk *recording* tetapi pengecekan dilakukan secara teratur.
   iii. Tidak ada prosedur atau dokumen untuk *maintaining* dan *approving* hak akses.

e. Tidak ada Prosedur atau dokumen untuk dilakukan perusahaan pada hak akses karyawan saat karyawan tersebut pindah pekerjaan, dipecat dan pindah jabatan.

4.4. Kesimpulan Evaluasi Kontrol

Rekapitulasi evaluasi kontrol adalah

- Kriteria "Tidak Efektif" = 1
- Kriteria "Efektif dengan Perbaikan Besar" = 10
- Kriteria "Efektif dengan Perbaikan Kecil" = 0
- Kriteria "Efektif" = 0.

Dengan melihat rekapitulasi evaluasi kontrol disimpulkan bahwakontrol yang dimiliki maka dapat disimpulkan sebagian besar efektif dengan perbaikan besar IT security PT X.

Karena kontrol yang dimiliki efektif dengan perbaikan besar, maka proses evaluasi prosesmenggunakan *compliance test*yaitumembandingkan antara proses sesungguhnya yang terjadi di lapanngan dengan kontrol.

4.4 Standar Penilaian Proses Berdasarkan *Control Practices*

Untuk standar penilaian evaluasi proses untuk *Control Practices* yang dipakai adalah *control Practices* yang sama dengan evaluasi kontrol, tetapi menggunakan standar penilaian yang berbeda. Perbedaan standar penilaian disesuaikan dengan tujuan evaluasi, yaitu mencari tahu apakah terdapat jaminan bahwa proses yang dijalankan oleh PT X selama ini akan mencapai *control Practices*, atau tidak.

Standar penilaian evaluasi proses adalah:

- *Assurance*

Proses dijamin memenuhi *control Practices* bila dilakukan dengan konsisten seperti waktu pelaksanaan audit.

- *Assurance with Modification*

Proses masih bisa dijamin dapat memenuhi *control Practices* bila dilakukan perubahan pada proses tersebut.

- *Non Assurance*

Proses tidak dijamin memenuhi *control Practices* karena pada saat dilakukan audit, proses tidak mampu menunjukkan kinerja yang menuju pencapaian *control Practices* tersebut. Proses yang mendapatkan penilaian ini perlu diberi penyesuaian seperti yang dijelaskan pada setiap bagian proses evaluasi.

4.5 Evaluasi Proses Berdasarkan *Control Practices*

Untuk evaluasi tidak dilakukan menggunakan kuesioner, tetapi penilaian berdasarkan dokumen yang dikumpulkan dan wawancara selama proses audit. Dokumen yang telah dikumpulkan, dinilai dan diberikan usulan untuk perbaikan sesuai dengan pemenuhan kriteria-kriteria COBIT DS 5 di bawah:

Kriteria DS5.11 : *ASSURANCE WITH MODIFICATION*
Dokumen yang dianalisa: • Tidak ada dokumen yang dianalisa, karena SOP pertukaran data yang sifatnya sensitif tidak oleh dilihat.
Keterangan evaluasi: Ada prosedur pertukaran dan transaksi data yang sensitif tetapi divisi IT tidak diperbolehkan melihat prosedurnya tetapi tidak ada bukti pengiriman, bukti penerimaan dan *non-repudiation* yang dijalankan PT X untuk pertukaran data yang sifatnya sensitif. Pembuataan infrastruktur jaringan yang mendukung kebijakan diatas sedang dikembangkan oleh PT X. Tiap *infrastructure* jaringan diberi subnet masing-masing.
Usulan Perbaikan: • Terapkan kontrol aplikasi yang sesuai untuk melindungi pertukaran data. • Terapkan kontrol infrastruktur yang tepat, berdasarkan klasifikasi informasi dan teknologi yang digunakan, untuk melindungi pertukaran data.

Tabel 4.11 Penilaian Kriteria Evaluasi Proses DS 5.11

4.6. Kesimpulan Evaluasi Proses

Rekapitulasi evaluasi proses adalah:

- Kriteria "*Assurance*" = 0
- Kriteria "*Assurance with modification*" = 7
- *Non Assurance* = 4

Dengan melihat rekapitulasi evaluasi proses disimpulkan bahwa proses yang dimiliki maka dapat disimpulkan sebagian besar kriteria yang terdapat adalah *Assurance with modification* di IT *security* PT X. Tetapi masih banyak pula yang masih berada di dalam kriteria *non assurance,* sehingga masih banyak perbaikan yang harus dilakukan oleh PT X agar dapat benar-benar dijamin (*assured*).

5. PENILAIAN MATURITY LEVEL

Untuk menentukan *maturity level* pada proses pengadaan aplikasi di PT X, maka *control objectives* pada proses DS5 perlu dijabarkan menjadi beberapa kriteria. Kriteria tersebut kemudian diberi prosentase yang menentukan bobot kriteria tersebut terhadap *maturity level* prosessecara keseluruhan.

Proses pengukuran dilakukan menggunakan kuesioner yang ditunjukkan pada lampiran. Hasil dari penyebaran kuesioner kemudian dikumpulkan, dikalkulasi menurut prosentase tingkat kepentingan.

Hasil akhir pengukuran *Maturity Level* saat ini adalah 1.7**.**

Hasil akhir pengukuran *Maturity Level* yang diinginkan adalah 4.4

Dari hasil pengukuran di atas diketahui bahwa *maturity level* IT security PT X masih jauh dari yang diharapkan dengan rata-rata masih berada pada *level* 1, atau 2. Pada level 1, atau 2 menunjukkan bahwa belum ada prosedur yang ditetapkan dan didokumentasikan yang menjadi standar operasi IT *security*. Hal ini menjadikan *level* pada proses ini sangat rendah. Untuk itu diperlukan cukup banyak perbaikan dalam proses IT *security* pada PT X agar dapat memenuhi *level* yang diinginkan, maka penulis berikan rekomendasi perbaikan yang harus dilakukan kepada PT X.

6. KESIMPULAN DAN SARAN

6.1. Kesimpulan

Secara menyeluruh IT security PT Xbelum dijamin untuk mencapai *control objectives*.

- Hampir seluruh efektif dengan perbaikan besar dan ada yang tidak efektif untuk menjaga IT *security* yang selama ini dijalankan agar mencapai kondisi ideal dari *control objectives.*
- IT *security* sendiri masih banyak memerlukan perbaikan hingga benar-benar dijamin (*assured*) dapat mencapai *control objectives*. Banyak proses masih mendapatkan status *assurance with modification*, dan empat proses mendapat status *non assurance*.
- Divisi IT perlu menetapkan surat tugas dan memberikan laporan bulanan yang diberikan kepada dewan bisnis dan yang paling penting adalah perlu dibuat sebuah set lengkap kebijakan dan standar keamanan yang sejalan dengan kerangka kebijakan keamanan informasi yang dimiliki PT X.
- Untuk manajemen *user* perlu mengkomunikasikan dengan semua *stakeholder* dan user secara tepat waktu dan teratur pada update informasi strategi keamanan, rencana, kebijakan dan prosedur, selain itu perlu menetapkan metode untuk otentikasi dan otorisasi pengguna untuk membangun tanggung jawab dan menegakkan hak akses sesuai dengan sensitivitas informasi dan fungsional. Perlu pula dibuat SOP tentang user seperti prosedur untuk user baru, otentikasi dan otorisasi, hak akses,dll.
- Untuk bagian keamanan software perlu dibuat prosedur untuk menegakkan kebijakan pencegahan software berbahaya dalam organisasi, perlu juga prosedur untuk memaksakan antivirus agar paling *update* dan tersentralisasi.
- Untuk Data dan informasi diharapkan segera menerapkan fungsi kriptografi untuk melindungi data dan informasi milik perusahaan, perlu membuat prosedur untuk menentukan langkah-langkah untuk melindungi kerahasiaan informasi yang berkaitan dengan *security incidents.*
- Buat persyaratan keamanan informasi yang dikumpulkan dari TI rencana taktis, klasifikasi data, standar teknologi , kebijakan keamanan dan kontrol , risiko manajemen, dan persyaratan eksternal untuk integrasi ke dalam rencana keamanan TI secara keseluruhan.
- Rencanakan arsitektur keamanan jaringan untuk menunjukan pengolahan dan persyaratan keamanan.
- Buat prosedur yang menetapkan, menjaga, mengkomunikasikan dan menegakkan kebijakan keamanan jaringan yang ditinjau dan diperbarui secara teratur setidaknya setahun sekali.

6.2. Saran

- Disarankan untuk segera membuat kendali mutu untuk sistem kendali mutu yang ada di PT X, karena kendali mutu yang baik dapat memperlancar dan memperjelas kinerja sistem kendali mutu yang dijalankan selama ini.
- Dalam pembuatan sistem kendali mutu, harus memperhitungkan IT *security* juga, karena IT security merupakan bagian yang tidak terpisahkan dari sistem kendali mutu.
- IT *security* merupakan bagian yang sangat penting untuk perusahaan, oleh karena itu perlu lebih ditingkatkan lagi investasi dan perhatian perusahaan terhadap IT *security* agar dapat memenuhi *control objectives* yang terdapat di dalam COBIT 4.1 DS 5 *Ensure System Security*.

7. DAFTAR PUSTAKA

[1] Gondodiyoto, S.& Hendarti, H. 2006 *Audit Sistem Informasi*,Jakarta: Erlangga.

[2] Indrajit, Richardus Eko. 2001. *Sistem Informasi dan Teknologi Informasi*. Jakarta:Gramedia.

[3] [ITGI] Information Technologi Governance Institute 2007. *COBIT 4.1 Edition:Guidelines, IT Governance Institute.* Illinois: ITGI.

[4] Ron,weber 1998 *The Information System Audit Process*, NJ: Prentice Hall.

[5] Sarno. R. 2009. *Strategi Sukses Bisnis dengan Teknologi Informasi.* Surabaya : ITS Press.

[6] Surendro, Kridanto 2009 *Implementasi Tata Kelola Teknologi Informasi . Bandung : Informatikan Bandung*