Audit Sistem Keamanan Jaringan Pada PT TRIAS SENTOSA TBK

Michael Setiono[1], Leo Willyanto[2], Agustinus Noertjahyana[3]
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) – 8417658
Email : m26412033@john.petra.ac.id[1], leow@petra.ac.id[2], agust@petra.ac.id[3]

ABSTRAK

PT Trias Sentosa didirikan pada tahun 1979. Perusahaan ini berurusan dengan manufaktur dan produksi plastik, Selama tahun terakhir sampai saat ini, PT. Trias Sentosa Tbk telah menggunakan sebuah sistem keamanan yang sangat terkendali dan sudah teruji kelayakanya dalam komunikasi antar tiap-tiap gudang ke server pusat. Akan tetapi, terkadang data dari BOPPET yang masuk ke server terkadang mengalami error atau yang sering di sebut "bug" hal ini menyebabkan adanya data yang terduplikat dan data yang kurang valid, padahal tiap harinya PT Trias sendiri membuat plastic dengan jumlah yang banyak. Maka dari itu, Audit Sistem Informasi & ISO (International Organization for Standardization) menjadi sebuah solusi untuk mengukur apakah keamanan dari sistem aplikasi yang ada dalam perusahaan tersebut sesuai dengan standar yang telah diakui secara internasional yaitu IT *governance* yang terdapat pada COBIT (*Control Objectives for Information and Related Technology*). COBIT merupakan sebuah kerangka kerja teknologi informasi yang dipublikasikan oleh ISACA (*Information System Audit and Control Association*) dan digunakan karena memiliki tingkat kompleksitas yang tinggi dan cakupan yang luas. Serta dalam analisa ini, domain yang digunakan berdasarkan COBIT adalah *Deliver & Support*. Lalu dari domain tersebut, pembahasan dibatasi pada tingkat DS5 *(Ensure Security Systems).* Dan untuk ISO sendiri dibatasi oleh ISO 27002 (*Information Security Management System.)*

Kata Kunci: *Sistem keamanan, Cobit 4.1, ISO 27002*

ABSTRACT

PT Trias Sentosa was founded in 1979. The company is dealing with manufacturing and production of plastics, During the last year to date, PT. Trias Sentosa Tbk has used a security system that is highly controlled and has been tested kelayakanya communication between each warehouse to a central server. However, sometimes the data from BOPPET that go into servers sometimes experience an error or what is often called "bugs" this causes their data and data terduplikat less valid, but each day PT Trias itself made of plastic with a large number. Therefore, the Information Systems Audit and ISO (International Organization for Standardization) to a solution to measure whether the security of application systems that exist within the company in accordance with the standards that have been internationally recognized that IT governance contained in the COBIT (Control Objectives for Information and Related Technology). COBIT is a framework for information technology published by ISACA (Information Systems Audit and Control Association) and is used because it has a high level of complexity and coverage. As well, in this analysis, the domain used is based on COBIT Deliver and Support. Then from that domain, the discussion is limited to the level DS5 (Ensure Security Systems). And to ISO itself is limited by ISO 27002 (Information Security Management System.) ***Keywords****: Network security, Cobit 4.1, ISO*

1. PENDAHULUAN

Teknologi dan sistem informasi di dunia semakin berkembang seiring dengan berjalannya waktu. Hampir semua kebutuhan dalam hidup manusia sudah dikaitkan dengan teknologi, mulai dari kebutuhan rumah tangga, edukasi, kesehatan, dan terlebih kegiatan perkantoran maupun perusahaan. Sehingga penting bagi suatu perusahaan untuk menerapkan teknologi yang sesuai dengan proses bisnis yang ada dalam perusaha an tersebut. PT. Trias Sentosa Tbk merupakan perusahaan multinasional terbesar di Indonesia yang memproduksi plastik yang bermarkas di Sidoarjo, Indonesia. Perusahaan ini didirikan pada 23 November 1979.Perusahaan ini menghasilkan plastik film berbahan Polypropelene dan Polyesther serta Metalizing, Coating dan Lamination. Total kapasitas produksi Perusahaan adalah 67,000 MT per tahun.

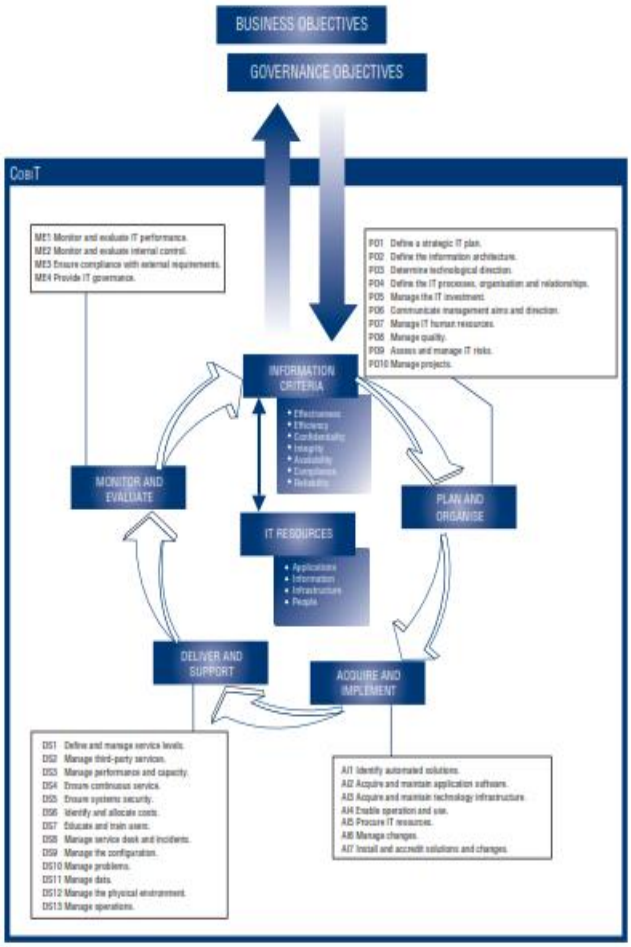
2. LANDASAN TEORI

2.1 Cobit 4.1

COBIT Framework adalah standar kontrol yang umum terhadap teknologi informasi, dengan memberikan kerangka kerja dan kontrol terhadap teknologi informasi yang dapat diterima dan diterapkan secara internasional. COBIT bermanfaat bagi manajemen untuk membantu menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan IT yang sering tidak dapat diprediksi. [1]

Kerangka kerja *Control Objectives for Information and related Technology* (COBIT) versi 4.1. COBIT versi 4.1 adalah model standar pengelolaan IT yang telah mendapatkan pengakuan secara luas, dikembangkan oleh Information Technology Governance Institute (ITGI) dari Information System Audit and Control Association (ISACA). Menurut IT Governance Institute, 2007, menyatakan bahwa pada versi 4.1 ini diuraikan good practices, domain-domain dan proses kerangka kerja (*framework*) TI yang ada. Selain itu versi 4.1 juga menjelaskan masalah pengelolaan proses TI dan bentuk-bentuk kegiatan (process and activity) dan mempunyai struktur yang sangat logis.

Berdasarkan IT Governance Institute (2012), Framework COBIT disusun dengan karakteristik yang berfokus pada bisnis (bussiness focused). Pada edisi keempatnya ini, COBIT Framework terdiri dari 34 high level control objectives dan kemudian mengelompokan proses tersebut menjadi 4 domain, keempat domain tersebut antara lain: Plannig and Organization, halAcquisition and Implementation, Delivery and Support, dan Monitoring and Evaluation: Hal tersebut bias kita lihat dalam gambar 1 yaitu tujuan dari Cobit sendiri.



Gambar 1 Cobit 4.1

2.2DS5 (*Ensure Security System*)

Klausul DS5(memastikan keaman sistem) sendiri memiliki 11 klausul yaitu hal tersebut berhubungan dengan sesuai dengan tujuan dari DS5 sendiri:

1. Manajememen Keamanan IT
2. Renacan keamanan IT
3. Manajemen Identitas
4. Manajemen Akun pengguna
5. Uji Coba keamanan, Penjagaan dan Pemantauan
6. Definisi Insiden Keamanan
7. Proteksi teknologi keamanan
8. Manajemen kunci kriptografi
9. Pencegahan software berbahaya, deteksi dan perbaikan
10. Keamanan jaringan
11. 'Pertukaran Data Sensitif

Hal tersebut dipilih untuk menjaga integritas informasi dan melindungi aset TI memerlukan proses manajemen keamanan. Proses ini meliputi penyusunan dan memelihara peranan-peranan keamanan (*security roles*) serta tanggung jawab, kebijakan, standar dan prosedur. Manajemen keamanan juga mencakup pengawasan keamanan dan ujicoba secara periodik, serta mengimplementasikan aksi perbaikan untuk kelemahan kekurangan atau insiden/bencana.

2.3 *ISO* 27002:2005

ISO 27002 merupakan salah satu standart keamanan informasi yang diterbitkan oleh ISO dan IEC(*International Electrotechnical Commission*). Standar ini merupakan penamaan ulang dari ISO/IEC 17799:2005. Standar ini dapat digunakan sebagai titik awal dalam penyusunan dan pengembangan ISMS. Standar ini memberikan panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset-aset informasi.Standar ini berisi 15 klausa kontrol keamanan yang secara bersama berisi 39 kategori keamanan utama dan satu klausul pengantar memperkenalkan penilaian resiko dan perlakuan. Masing-masing klausa terdiri dari sejumlah kategori keamanan utama. Masing-masing kategori keamanan utama terdiri dari tujuan kontrol yang menyatakan apa yang ingin dicapai dan satu atau lebih kontrol yang dapat diterapkan untuk mencapai tujuan kontrol. Berikut adalah 11 section yang terdapat dalam ISO 27002::2005: [3]

- *Security Policy*
- *Organization Of Information Security*
- *Asset Management*
- *Human Resourses Security*
- *Physical And Environmental Security*
- *Communications And Operations Management*
- *Access Control*
- *Information Systems Acquisition, Development And Maintenance*
- *Information Security Incident Management*
- *Buisness Continuity Management*
- *Compliance*

3. AUDIT DALAM PERUSAHAAN

3.1 Metode Audit

Berdasarkan persetujuan dari pihak perusahaan, penulis melakukan penelitian yaitu audit sistem informasi berdasarkan ruang lingkup, metode dan persetujuan waktu yang diajukan oleh perusahaan. Namun ada beberapa hal yang tidak boleh di dokumentasikan seperti foto dari data yang menyangkup bisnis proses dikarenakan oleh sensitifnya informasi. Berikut adalah aktivitas yang dilakukan oleh penulis untuk melakukan audit sistem informasi:

- Observasi dan Interview: Aktivitas dilakukan penulis untuk mengumpulkan bukti yang digunakan untuk memberikan masukan, penilaian serta rekomendasi pada perusahaan. Observasi ini dilakukan dalam beberapa aspek, yaitu: Bentuk dari jaringan dan topologi khususnya di bidang keamanan IT itu tersendiri. Selain itu dalam interview juga peneliti melakukan tanya jawab dengan beberapa narasumber dari perusahaan tersebut.
- Hasil Observasi dan laporan : Berdasarkan penelitian yaitu pelaksanaan audit sistem keamanan jaringan pada PT Trias, maka peneliti di akhir penelitian akan menulis suatu laporan mengenai hasil penelitian tersebut. Hasil penelitian tersebut nantinya akan membahas kondisi terkini yang sedang terjadi dalam perusahaan. Selain kondisi terkini, peneliti juga membahas tentang bukti temuan audit, temuan adalah hasil dari pelaksanaan dari metode penelitian yang digunakan peneliti. Temuan tersebut nantinya akan dibahas dalam rekomendasi untuk perusahaan sehingga perusahaan dapat memperbaiki tata kelola IT berdasarkan rekomendasi dari peneliti.

Audit akan ada tinjauan pustaka dari ISO 27002 dan DS5 yang telah dipilih oleh penulis sebagai dasar dari audit itu sendiri. Setelah tinjauan pustaka dari situ penulis membuat sebuah kuisioner berdasarkan tujuan dari tinjauan pustaka sendiri, baru setelah itu

kuisioner akan di tanyakan dengan cara wawancara dan nantinya pihak yang diwawancarai harus menunjukan bukti bahwa klausa tersebut sudah sudah di implementasikan atau belum. Setelah penulis menerima jawaban, penulis akan melakukan studi lapangan untuk memastikan bahwa apa yang dikatakan itu benar sudah dilakukan atau belum dan dari kedua proses ini maka penulis akan membuat laporan yang berisi hasil dari audit serta menyetarakan saran, kritik dan rekomendasi dalam bidang keamanan jaringan untuk perusahaan.

4. HASIL AUDIT

4.1 DS5 (Ensure Security System)

1. DS5.1 Management of IT Security: Efektif dengan perbaikan besar
   a. Tugas untuk divisi IT hanya diberitahu secara lisan dan tidak dicatat dan tidak ada surat tugas.
   b. Tidak ada laporan rutin
   c. Struktur organisasi terstruktur berdasarkan struktur perusahaan
2. DS5.2 IT Security Plan: Efektif dengan perbaikan besar
   a. Analisa kontrol 5.2a:
      i. IT policy sudah ada tapi belum lengkap dan hanya formailitas saja tidak menyangkup mengenai keamanan
      ii. SOP belum ada
      iii. Belum ada dokumen atau catatan yang megakan standart keamanan
      iv. Belum ada peraturan dan standart prosedur untuk praktek penegakan pelangaran Standar Keamanan perusahaan, bila terjadi kesalahan hanya ditegur secara lisan saja.
      v. Untuk investasi kemanan IT sendiri perusahaan menggunakan CCTV, fingerprint dan perangkat jaringan yang bermutu.
   b. Analisa kontrol 2.2b:
      i. Rencana IT ke depan adalah untuk mendapatkan sertifikasi di bidang ISO, mereka sedang menyiapkan diri sebagai contoh mereka sedang berusaha menerapkan enkripsi.
      ii. Klasifikasi data sudah ada.
      iii. Standar teknologi belum ada
      iv. Kebijakan keamanan beberapa ada seperti kebijakan Email
      v. Manajemen resiko belum ada.
      vi. Memiliki perjanjian untuk pihak luar. akan tetapi kadang hanya diberi tahus ecara lsian saja, karena dibertahu secara lisan sudah cukup.
   c. Analisa kontrol 2.3c:
      i. Untuk software dan hardware selama ini berjalan dengan baik dan memiliki mutu yang cukup untuk pusat data atau server.
      ii. Infrastruktur dan topologi dari jaringan sudah tertata dengan baik cuma terkadang kalau kita lihat di lapangan, tempat penataan router dan kabel jairngan kurang efektif.
   d. Sudah memeiliki kebijakan mengenai stakeholder dan user akan tetapi tidak didokumentasikan hanya sosialisasi saja dan diberitahu secara lisan
3. DS 5.3 Identity Management: Efektif dengan perbaikan besar
   a. Analisa kontrol untuk DS 5.3a
      i. Untuk proses identifikasi user di gunakan secara unik menggunakan alat fingerprint dan suara yang ada di sebuah mesin terletak di depan receptionist.
      ii. Belum ada dokumen untuk mekanisme otoritas dan otentifikasi hanya dilakukan secara aktual akan tetapi tiap karywan sudah di berithu secara lisan
      iii. Hak akses di simpan dalam SAP
   b. Analisa kontrol untuk 5.3b
      i. Sensitifitas informasi dan aplikasi yang terlibat diperhitungkan oleh perusahaan, namun belum di catat dan di dokumentasikan
      ii. Belum ada kebijakan untuk perlindungan informasi dan juga belum ada peraturan yang menyangkut hukum. Akan tetapi tiap karyawan sudah deiberitahu secara lisan mengenai pentingnya informasi
      iii. Sudah ada dokumen di IT policy untuk pembagian hak akses sesuai peran dan tanggung jawab akan tetapi belum di definisikan secara jelas dalam dokumen tersebut.
      iv. Hak akses diberikan sesuai kebutuhan dan peran tiap user beberapa sudah di dokumentasikan tapi beberapa belum.
      v. Belum ada prosedur persyaratan untuk pemisahan tugas yang tepat.
   c. Belum ada prosedur otoritasi untuk menetapkan tanggung jawab dan menegakan hak akses sesuai dengan pentingnya informasi. Tetapi sudah diberitahu secara lisan.
   d. Analisa kontrol untuk DS 5.3d:
      i. Tidak ada prosedur atau dokumen mengenai user yang baru hanya di breefing secara lisan saja.
      ii. Belum ada prosedur atau dokumen untuk maintaining dan approving hak akses.
   e. Sudah ada prosedur untuk dilakukan perusahaan pada hak akses karyawan saat karyawan dipecat atau pindah jabatan
4. DS 5.4 User Account Management: Efektif dengan perbaikan besar
   a. Analisa kontrol untuk DS 5.4a:
      i. Sudah ada prosudur yang mengatur unique ID
      ii. Belum ada prosuder yang mengatur group ID
   b. Analisa kontrol untuk DS 5.4b:
      i. Untuk penutupan user account diatur dalam SAP
      ii. Untuk permintaan user account diatur dalam SAP
      iii. Untuk modifikasi yang dilakukan oleh user juga di monitoring oleh SAP
   c. Belum ada sebuah prosedur yang mengatur system untuk memeriksa apakah user sesuai dengan otorisasinya, sistem dari SAP cuma bisa melihat saja. Namun di dalam IT *policy* sudah tercantum otoritasnya.
   d. Analisa kontrol untuk DS 5.4d:
      i. Belum ada prosedur atau dokumen mengenai maintenance terhadap data-data
   e. Untuk arus informasi untuk melaporkan perubahan dalam pekerjaan tentang hak akses cukup baik yaitu 24 jam setelah ada perubahaan.
5. DS 5.5 Security Testing, Surveillance and Monitoring: Efektif dengan perbaikan besar

a. Belum ada prosedur atau dokumen untuk mengatur pengujian security secara berkala
b. Analisa kontrol DS 5.5b:
   i. Belum ada prosedur atau dokumen untuk mengatur identity management tetapi dilakukan oleh perusahaan secara berkala
   ii. Belum ada dokumentasi atau prosedur untuk security monitoring tetapi dialukan terus dalam perusahaan
   iii. Belum ada prosedur atau dokumen untuk batasan atau konfogurasi sistem
   iv. Belum ada dokumentasi untuk memvalidasi bahwa jaringan sudah aman dan terkonfigurasi secara benar, akan tetapi perusahaan terus meningkatkan kinerja agar bisa meningkatkan keamanan dalam bidang IT
   v. Tidak ada dokumen untuk review dari konsultan, tetapi konsultan terus memberi saran demi kemajuan IT dalam perusahaan.

6. DS 5.6 Security Incident Definition: Efektif dengan perbaikan besar
   a. Selama ini belum ada dokumen atau catatan mengenai insiden dalam hal kemanan IT dalam perusahaan karena masalah selama ini ada bisa diselsaikan secara mudah.
   b. Belum ada dokumen mengenai bagaimana mengatasasi insiden
   c. Perusahaan berusaha untuk melindungi informasi dengan cara memberitahu karywaanya untuk tidak menempelkan media seperti HP, USB sembarangan di pusat data.
7. DS 5.7 Protection of Security Technology: Efektif dengan perbaikan besar
   a. Analisa kontrol DS5.7a:
      i. Belum ada prosedur atau dokumen yang mengatur secara berkala terhadap keamanan IT pada perusahaan agar tidak mudah dirubah orang.
      ii. Belum ada prosedur atau dokumen yang mengatur untuk mengamankan dokumen dari pihak luar namun tiap karywan sadar mengenai pentingnya
      iii. Belum ada prosedur atau dokumen yang mengatur agar dokumen tidak mudah dibongkar.
   b. Dalam uji mekanisme di tiap update terkadang tidak diuji.dan jarang untuk melakukan update
8. DS 5.8 Cryptographic Key Management: Efektif dengan perbaikan besar
   a. Sudah ada implementasi untuk enkripsi data dalam bidang email dengan menggunakan microsoft exchange untuk kriptografinya di atur oleh microsoft sendiri.
9. DS 5.9 Malicious Software Preventation, Detection and Correction: Efektif dengan perbaikan besar
   a. Selama ini perusahaan belum mendapati masalah mengenenai malware jadi belum berpengalaman untuk hal tersebut.
   b. Analisa kontrol DS 5.9b:
      i. Tidak ada prosedur atau dokumen yang memaksakan agar antivirus selalu ter up-to-date, tetapi kenyataanya antivirus yang dimilik selalu paling update.
      ii. Memang tidak ada dokumentasi atau prosedur yang mengharuskan antivirus terinstal, tapi tiap komputer pada perusahaan sudah terinstall antivirus yang cukup bagus.
10. DS 5.10 Network Security: Efektif dengan perbaikan besar
    a. Belum ada prosedur atau dokumentasi mengenai filter sehingga aman dari akses yang tidak resmi
    b. Belum ada dokumen mengenai penanganan semua komponen jaringan pada perusahaan, terkadang pada prakteknya jaringan banyak yang tidak terkontrol dengan baik.
    c. Monitoring hanya dilakukan untuk melindungi perangkat dari serangan, hal ini dilakukan tiap 1 bulan sekali tetapi tidak ada dokumentasi dan prosedurnya.
    d. Konfigurasi dari OS di peursahaan meminimalisir dan melakukan uninstall terhadap fitur dan aplikasi yang dianggap tidak penting.
    e. Topologi dan arsitektur sudah ada dan sudah di dokumentasikan topologinya.
11. DS5.11 Exchange of Sensitive Data: Efektif dengan perbaikan besar
    a. Sudah ada prosedur dan dokumentasinya mengenai pertukaran data yang sensitif menggunakan jalur yang khusus. Akan tetapi perusahaan masih belum bisa menjelaskan teknologinya karena masih dalam tahap perbaikan.
    b. Untuk pengiriman memang belum ada bukti dan dokumentasinya dalam pengiriman dan bukti penerimaan dalam pertukaran data yang sensitif
    c. Untuk kebijakan belum ada dokumentasinya dan perusahaan sedang berusaha membuatnya.[4]

4.2 ISO 27002:2005

Klausul 1:

Menurut perusahaan sendiri keamanan merupakan hal yang penting karena menyangkut kerahasian perusahaan dalam data, namun masih ada kurang.nya sosialisi akan pentingnya keamanan data dan jaringan karena mereka masih belum berpengalaman dan selama ini belum terjadi insiden. Untuk strategi bisnis dan tujuan manajemen sendiri memiliki bebrapa tujuan salah satunya adalah membuat perusahaan ini menjadi go internasional dan memiliki standar yang bagus. Untuk IT *policy* sudah ada namun hanya 3 halaman dan tidak menyangkup semuanya di dalam nya hanya terdapat tanggung jawab mengenai fasilitas dan tanggung jawab yang mereka dapatkan.

Klausul 2:

Untuk dokumentasi dari tujuan dari keamanan informasi memang sudah ada namun banyak dari karyawan yang masih tidak mengerti pentingnya keamanan padahal keamanan informasi bukan hanya diurus pihak IT saja. Untuk *security* policy belum ada hanya diberitahu secara lisan aja. Karena tidak ada *security* policy maka kesadaran akan pentingnya keamanan belum timbul serta untuk keamanan informasi sudah di sosialisasikan misal: semua orang tidak boleh masuk ke pusat data atau server. semua orang sudah tahu, namun terkadang orang IT sendiri teledor terkadang lupa untuk menutup pintu masuk/keluar server

Klausul 3:

Untuk dokementasi dari aset ini masih sudah ada namun sedang diusahakan untuk diperbaiki lagi agar menjadi lebih baik. Penggunaan dari aset perusahaan seperti email dan internet juga

dibatasi dengan IT *policy* dimana tiap karywan dilarang keras untuk menggunakan internet untuk pornigrafi dan sosial media

Klausul 4:

Untuk kebijakan keamanan informasi sudah ada namun belum di dokumentasikan, namun kebijakan secara lisan itu sudah menjelaskan mengenai hak akses dan resiko jika ditemui melakukan pelanggaran dalam bidang keamanan misal: meng otak-atik settingan dari server atau router tanpa seijin pihak IT akan dikenakan sanksi atau teguran. Untuk pengecekan tiap karyawan secara rahasia sudah dilakukan bekerja sama dengan pihak HRD dengan begitu perusahaan mengertai mengenai *background* dari beberapa karyawan nya namun hal ini tidak mungkin di dokumentasikan karena mengingat bahwa ini bersifat pribadi. Untuk sementara untuk hak akses sudah di bagi menurut pekerjaan mereka.

Klausul 5:

Dalam hak akses karywan sudah mengerti mengenai hak akses mereka namun belum ada dokumentasinya untuk hal itu, serta untuk parameter dalam hal keamanan perusahaan menggunakan pembatasan dalam hal masuk ke pusat data atau server hingga saat ini hanya 4 orang saja yang boleh masuk ke ruang server dan untuk masuk ke ruang UPS hanya 3 orang,

Klausul 6:

Untuk prosedur untuk menghandle sistem informasi yang banyak ini maka dari itu di dalam IT ada sebuah tim yang dibentuk untuk menangani banyaknya informasi ini. untuk prosedur backup sudah ada prosedur namun belum ada dokumentasinya. system log sudah ada sehingga bisa monitoring. jika ada perubahan prosedur pasti dilakukan testing terlebih dahulu sehingga meminimalisir resiko sistem gagal dalam testing ini biasanya menggunakan *dummy* dulu tidak langsung di test dalam perangkat lunak. dan juga para editors dan development tidak diperbolehkan untuk masuk ke dalam system karena, system sendiri bersifat rahasia.

Klausul 7:

Untuk tiap user ID sudah menggunakan *unique* ID sehingga tiap user sudah dapat bertanggung jawab dengan ID.nya masing-masing namun kalau group ID masih sedang berusaha untuk di implementasikan Untuk dokumentasi mengenai kebijakan belum ada. Untuk *privileges* tiap user sudah ada sebenarnya dalam prosedural namun belum ada dokumentasinya. Password yang digunakan tiap karyawan sudah ada namun mudah ditebak dan perusahaan mengharuskan tiap karyawan untuk mengganti password setiap 1 bulan sekali, namun tidak dilakukan oleh karyawan.

Klausul 8:

Setiap bisnis transaksi sudah di input mulai dari nama, alamat dan cara pembayaran dari pembeli, namuan belum ada proses untuk mengecek apakah data itu valid misal: nama tidak boleh huruf. sehingga tiap user yang menginput data harus teliti dan untuk yang memonitoring dan maintance juga jarang dilakukan. Untuk data transaksi hanya pihak dari keuangan saja yang bisa mengecek dan pihak HRD.

Klausul 9:

Untuk insiden yang menyerang keamanan seperti *malicious* dan virus semuanya tidak ada dokuemntasinya, namuan sudah ada prosedur dan jika ada insiden begini karywan hanya lapor ke atasan. selama ini belum ada yang menganalisa untuk kelemahan dari keamanan. Jika terjadi insiden yang menyebabkan hilangnya data, perusahaan masih ada belum backupnya namun hal itu bisa jadi menggangu bisnis proses karena mengunggu proses *recovery*

Klausul 10:

Untuk proses dan prosedur ini perusahaan masih memikirkan untuk kedepanaya, namun jika terjadi bencana alam yang tidak terduga yang menyebabkan hilangnya data, perusahaan belum mempunyai backup yang ada sehingga data akan hilang semua dan fasilitas mail langsung hilang dan tidak dapat diakses.

Klausul 11:

Tiap manager dan karywan masih belum mengerti pentingnya keamanan dalam bidang IT dan standar apa saja yang ada di perusahaan, padahal kenyataanya paling tidak perusahaan sudah menerapkan standar yang cukup contoh: K3(Kesehatan dan keselamatan kerja) [5]

5. KESIMPULAN & SARAN

Berdasarkan audit yang dilakukan pada perusahaan bisa dilihat bahwa sudah banyak prosedur yang sudah dilakukan, namun masih belum ada dokumentasi untuk prosedur tersebut, oleh karena itu perlu di dokumentasikan, dokumentasi ini bertujuan agar mengurangi konflik dan memprjelas proses implementasi dari proses sehingga hal itu membuat tiap karywan mengerti apa proses dan standar yang ada di perusahaan, serta tanggung jawab mereka sebagai karywan yang bekerja di perusahaan

Untuk di perusahaan lebih cocok untuk menggunakan standar dari ISO 27002:2005 karena iso sendiri merupakan standar international yang diakui oleh banyak negara jika perusahaan bisa sertifikasi dan mendapatkan sertifikasi nya maka akan banyak *customer* yang datang dan proses bisnis dapat meningkat secara derastis, namun dalam hal ini Cobit 4.1 DS5 juga bagus namun masih mendetail ISO 27002.

Berdasarkan hasil audit keamanan sistem informasi telah dilakukan, didapatkan pernyataan bahwa pihak perusahaan belum pernah diaudit dengan standar-standar lain. Untuk itu dapat dilakukan audit sistem informasi menggunakan standar lain selain ISO. [2]

6. DAFTAR PUSTAKA

[1] Moeller, R. R. 2013. Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Haboken: John Wiley and Sons, Inc.

[2] Moedjiono,Sadikin 2012. Perlindungan dalam hal aset-asset informasi.[internet].(http://moedjionosadikin.wordpress.com/2010/05/04/perlindungan-aset-asset- informasi/)

[3] ISO/IEC 27002:2005, 2007. Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005 - Final Draft. Switzerland: ISO/IEC JTC 1.

[4] Information Technology Governance Institute. (2007). COBIT 4.1 Edition: Audit Guidelines, IT Governance Institute. Illinois: ITGI.

[5] ISOa. 2005. International Standard ISO/IEC 17799 Information Technology - Security Technique - Code Of Practice For Information Security management. Geneva: International Standard Organization.