ISSN 2085-4579

Audit Sistem Informasi Menggunakan Cobit 4.1 pada PT. Erajaya Swasembada, Tbk.

Wella, Johan Setiawan
Program Studi Sistem Informasi, Universitas Multimedia Nusantara, Tangerang, Indonesia
wella.ict@umn.ac.id, johan@umn.ac.id

Diterima 4 Desember 2015
Disetujui 18 Desember 2015

Abstract – Main priority aspects of information and communication technologies is given to a control or control mechanisms, both internal and external, to ensure that the report and the decision received and generated by the management decision-making is an honest and have high integrity based on the results of the audit conducted on based systems of information and communication technology.

The object of research is the PT Erajaya Swasembada, Tbk. This company was founded in 1990, running a business as a distributor of mobile phones, which have widespread outlets in various cities in Indonesia. Business processes studied include sales, purchasing, finance, and the warehouse. The system used is "Erajaya Live Application Server" version of the July-December 2012 and based ERP (Enterprise Resource Planning).

The research was including a General Controls, Boundary Controls, Input Controls, Process Control, Output Controls, Database Control, Application Communication control, and Operating system controls. Data collection methods by performing interviews with the IT managerial departments, distributed questionnaires to the five respondents form of answer was "Yes", "No" or "Do not Know", and also observations to the PT Erajaya Swasembada, Tbk. The collected data were analyzed using techniques COBIT 4.1.

The results obtained 15 audit findings. The results of maturity model formulation were known domain Plan and Organize at level 4, Acquire and Implement at level 5, Deliver and Support at level 4, Monitor and Evaluate at level 4.

Index Terms- Audit, COBIT 4.1, Maturity Model.

I. Pendahuluan

Seiring dengan perkembangan ilmu pengetahuan dan teknologi, terjadi perpaduan antar dua bidang ilmu, khususnya pada bidang teknologi sistem informasi dan bidang akuntansi dengan spesifikasi audit sehingga menghasilkan bidang ilmu baru yaitu audit sistem informasi. Meskipun bidang ilmu ini baru muncul ke permukaan, tetapi sepak terjangnya sangat dibutuhkan. Perusahaan-perusahaan besar sangat membutuhkan peranan audit sistem informasi untuk memeriksa kehandalan dari sistem komputerisasi yang mereka gunakan dalam pengerjaan operasional perusahaan.

Dunia bisnis pada masa sekarang sangat mengandalkan teknologi informasi dan komunikasi untuk menjalankan proses bisnisnya. Oleh karena itu, adalah suatu hal yang penting bagi dunia bisnis untuk memahami dan mengerti aspek teknologi informasi dan komunikasi untuk dapat menerapkannya baik secara manajerial maupun teknikal pada proses bisnis dan kegiatan ekspansinya [1].

Pritoritas utama diberikan terhadap suatu mekanisme kontrol atau pengendalian, baik intern maupun ekstern, untuk memastikan bahwa laporan dan keputusan yang diterima dan dihasilkan oleh manajemen merupakan suatu pengambilan keputusan yang jujur dan mempunyai integritas tinggi berdasarkan hasil proses audit yang dilakukan terhadap sistem berbasis teknologi informasi dan komunikasi organisasi bisnis yang bersangkutan.

Adapun tujuan yang diinginkan dari audit sistem informasi ini adalah untuk menciptakan *Good Corporate Governance* di dalam suatu

perusahaan. Pengendalian internal masa depan, tidak hanya cukup dengan pengendalian umum (*general controls*) dan pengendalian aplikasi dan formulir (*application controls*), melainkan dibutuhkan juga pengendalian batasan (*boundary control*), pengendalian proses (*process control*), dan pengendalian komunikasi aplikasi (*application communication control*).

Salah satu standar penting dan efektif untuk diterapkan adalah COBIT atau *Control Objectives for Information and Related Technology*. COBIT dikeluarkan oleh organisasi bernama ISACA pada tahun 1992 dan merupakan standar yang berorientasi pada proses, berfokus pada sasaran bisnis dan merupakan alat manajerial dan teknikal untuk unit TI. Penelitian ini mengambil analisis keamanan dan integritas sistem informasi dengan menggunakan pengukuran COBIT 4.1 untuk mendukung tujuan bisnis tersebut [2].

Penggunaan bantuan dan metode COBIT, memberi manfaat untuk perusahaan yang dapat membantu untuk menciptakan *Good Corporate Governance* di dalam suatu perusahaan serta membantu auditor, manajemen dan pengguna (*user*) untuk menjembatani GAP antara risiko bisnis, kebutuhan kontrol (*internal, application and access control*), *security* dan permasalahan-permasalahan teknis melalui pengendalian terhadap masing-masing dari proses IT, serta meningkatkan tingkatan kemapanan proses dalam IT dan memenuhi ekspektasi bisnis dari TI.

II. TINJAUAN PUSTAKA

A. Definisi Audit Sistem Informasi

Berikut ini adalah pengertian Audit Sistem Informasi menurut beberapa ahli:

- Menurut Cangemi [3],

  "Information systems auditing is defined as any audit that encompass the review and evaluation of all aspects (or any portion) of automated information processing systems, including related non-automated processes, and the interfaces between them".

- Gondodiyoto [1] berpendapat bahwa,

  "Audit sistem informasi merupakan suatu pengevaluasian untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis, memiliki mekanisme pengamanan asset yang memadai, serta menjamin integritas data yang memadai".

- Menurut Hall [4],

  "*An IT Audit focuses on the computer-based aspects of an organization's information system. This audit includes assessing the proper implementation, operation, and control of computer resources. Because most modern information systems employ information technology, the IT audit is typically a significant component of all external (financial) and internal audits."*

Dari pengertian-pengertian para ahli mengenai Audit Sistem Informasi dapat disimpulkan menjadi, proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktiva dilindungi dengan baik / tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer. Evaluasi tersebut dapat dilakukan bersamaan dengan audit laporan keuangan, audit internal, atau bentuk lain dari keterlibatan pembuktian.

B. Pendekatan Audit Sistem Informasi

Menurut Weber [5], metode pendekatan audit sistem informasi antara lain adalah:

1. *Auditing around the computer*. Merupakan suatu pendekatan audit dengan memperlakukan komputer sebagai *black box*, maksudnya metode

ini tidak menguji langkah-langkah proses secara langsung, tetapi hanya berfokus pada input dan *output* dari sistem komputer. Diasumsikan bahwa jika input benar akan diwujudkan pada *output*, sehingga pemrosesannya juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.

2. *Auditing through the computer*. Merupakan suatu pendekatan audit yang berorientasi pada komputer dengan membuka *black box* dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Dengan asumsi bahwa apabila pemrosesan mempunyai pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi, sebagai akibat dari keluaran dapat diterima.
3. *Auditing with the computer*. Pendekatan ini dilakukan dengan menggunakan komputer dan *software* untuk mengotomatisasi prosedur pelaksanaan audit. Pendekatan ini merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas file dan *record* perusahaan. *Software* audit yang digunakan merupakan program komputer auditor untuk mebantu dalam pengujian dan evaluasi kehandalan data, file dan *record* perusahaan.

C. Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi secara garis besar terbagi menjadi 4 tahap yaitu [5]:

1. Meningkatkan keamanan aset-aset perusahaan. Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, file data harus dijaga oleh suatu sistem pengendalian intern yang baik aga tidak terjadi penyalahgunaan *asset*.
2. Meningkatkan integritas data. Integritas data (*data integrity*) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan, kebenaran, dan keakuratan.
3. Meningkatkan efektifitas sistem. Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem infromasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan *user*.
4. Meningkatkan efisiensi sistem. Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai.

Gondodiyoto [1] menyimpulkan tujuan audit sistem informasi sebagai berikut:

1. Pengamanan Aset, Aset informasi suatu perusahaan seperti *hardware, software*, sumber daya manusia (*brain ware*), file data harus dijaga oleh suatu sistem pengendalian internal yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal fundamental yang sangat penting yang harus dipenuhi oleh perusahaan.
2. Menjaga Integritas Data. Integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan, dan keakuratan. Jika tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki informasi atau laporan yang benar bahkan perusahaan dapat menderita kerugian darikesalahan dalam membuat atau mengambil keputusan.
3. Efektifitas Sistem, Efektifitas sistem perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan *user*.
4. Efisiensi Sistem. Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas

yang memadai. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minimal.

5. Ekonomis. Ekonomis mencerminkan kalkulasi untuk rugi ekonomi (*cost/benefit*) yang lebih bersifat kuantifikasi nilai moneter (uang).

Dari berbagai definisi diatas penulis menyimpulkan bahwa tujuan utama audit sistem informasi adalah untuk mengetahui dan menentukan apakah suatu sistem informasi yang berbasis komputer telah:

1. Memberikan perlindungan terhadap aset perusahaan.
2. Meningkatkan integritas data.
3. Meningkatkan efektifitas perusahaan dalam mencapai tujuannya.
4. Memungkinkan perusahaan menggunakan sumber dayanya secara efisien.

D. Tahapan Audit

Dalam melakukan kegiatan audit, peneliti memakai tahapan audit sebagai berikut [6]:

1. *Planning*, mendapatkan pemahaman yang lengkap mengenai bisnis perusahaan yang sedang dilakukan audit. Pada proses ini auditor menentukan ruang lingkup dan tujuan pengendalian, tingkat materialitas, dan *outsourcing*. Pada tahap ini auditor menetapkan mengapa, bagaimana, kapan dan oleh siapa audit akan dilaksanakan. Untuk mematangkan tahap perencanaan, sebuah program audit awal dipersiapkan untuk menunjukkan sifat, keluasan, dan waktu prosedur-prosedur yang dibutuhkan untuk mencapai tujuan audit dan untuk meminimalkan risiko-risiko audit.

2. *Prepare Audit Program*, audit program disesuaikan dengan hardware dan *software* yang dimiliki perusahaan, topologi dan arsitektur jaringan, dan lingkungan serta pertimbangan khusus mengenai industri tersebut. Komponen-komponen dari audit program tersebut adalah: ruang lingkup audit, sasaran audit, prosedur audit, dan rincian administratif (perencanaan dan pelaporan).

3. *Gather Evidence*, bertujuan untuk mendapatkan bukti-bukti memadai, handal, relevan, dan berguna untuk mencapai sasaran audit secara efektif. Jenis bukti yang sering ditemukan auditor pada kerja lapangan yaitu: observasi proses-proses dan keberadaan dari item fisik seperi pengoperasian komputer atau prosedur backup data, bukti dalam bentuk dokumen (seperti *program change logs*, sistem *access logs*, dan tabel otoritas), gambaran dari perusahaan seperi *flowcharts*, narratives, dan kebijakan dan prosedur yang tertulis), serta analisa seperti prosedur CAATs yang dijalankan pada data perusahaan.

4. *Form Conclusion*, mengevaluasi bukti-bukti dan membuat suatu kesimpulan tentang hasil pemeriksaan yang pada akhirnya akan mengarah pada opini audit. Auditor juga akan melaporkan kelemahan dan kelebihan dari sistem.

5. *Deliver Audit Opinion*, informasi umum yang harus ada dalam sebuah laporan audit yaitu:

a. Nama dari organisasi/perusahaan yang diaudit
b. Judul, tanda tangan, dan tanggal
c. Pernyataan sasaran audit dan apakah audit tersebut telah memenuhi sasaran
d. Ruang lingkup audit, termasuk

didalamnya area audit fungsional, periode audit yang tercakup, dan sistem informasi, aplikasi, atau lingkungan proses yang diaudit

e. Pernyataan bahwa telah terjadi pembatasan ruang lingkup dimana auditor tidak dapat melaksanakan pekerjaan audit dengan memadai untuk mencapai sasaran-sasaran audit tertentu

f. Pengguna laporan audit yang dikehendaki, termasuk beberapa pembatasan dalam pendistribusian laporan audit

g. Standar-standar dan kriteria yang menjadi dasar auditor untuk melaksanakan pekerjaan audit tersebut

h. Penjelasan rinci mengenai temuan-temuan penting

i. Kesimpulan dari area audit yang dievaluasi, termasuk di dalamnya syarat dan kualifikasi penting

j. Saran-saran yang tepat untuk tindakan perbaikan dan peningkatan

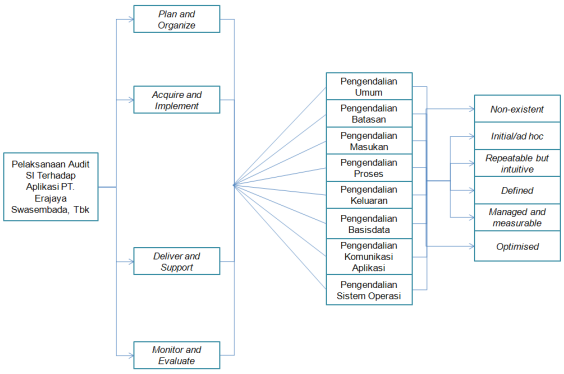
k. Peristiwa-peristiwa penting yang terjadi setelah masa *fieldwork* audit yang bersangkutan berakhir

6. *Follow Up,* melakukan tindak lanjut dengan membuat suatu ketentuan untuk melakukan tindak lanjut bersama dengan perusahaan pada kondisi-kondisi yang dilaporkan atau defisiensi audit yang tidak ter-*cover* selama kegiatan audit. Tindak lanjut ini dapat dilakukan dengan menelepon pihak menejemen.

E. Pengertian COBIT

COBIT merupakan cara atau metode yang dapat ditempuh untuk dapat menganalisa, mengembangkan, mempublikasikan, dan mempromosikan suatu otorisasi. COBIT ini dapat membuat *up-to-date* suatu sistem perusahaan serta dapat diterima oleh tata kelola TI profesional. Tata kelola TI yang dikontrol dibawah naungan COBIT merupakan tata kelola TI bertaraf internasional.

F. Kerangka Pikir



Gambar 1. Kerangka Pikir

Penelitian ini dilakukan untuk melihat bagaimana penerapan kinerja departemen TI perusahaan ditinjau dari pengendalian aplikasi "*Erajaya Live Application Server*" dalam proses ERP yang dijalankan pada PT Erajaya Swasembada, Tbk dan kesiapan departemen TI dalam melaksanakan proses-proses TI.

Adapun langkah awal dari penelitian ini adalah melakukan studi kepustakaan yaitu pembelajaran mengenai audit sistem informasi, khususnya mengenai metode audit COBIT 4.1, yang mencakup *Plan and Organise, Acquire and Implement, Deliver and Support, dan Monitor and Evaluate.*

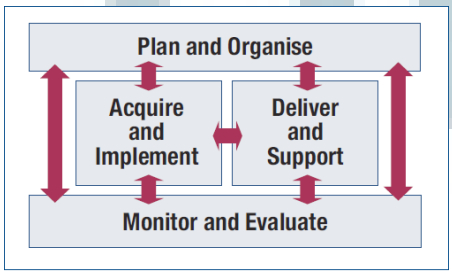
Langkah kedua dari penelitian ini adalah melakukan perencanaan pemeriksaan, yaitu melakukan observasi awal; merumuskan masalah yang akan diteliti; dan mengajukan permohonan penelitian kepada pihak terkait. Langkah ketiga dari penelitian ini adalah melakukan penelitian pendahuluan, yaitu merumuskan program audit yang akan dijalankan. Langkah keempat dari penelitian ini adalah melakukan identifikasi dan analisis masalah, yaitu menganalisa efektivitas pelaksanaan pengendalian aplikasi. Langkah kelima dari penelitian ini adalah melakukan pelaksanan pemeriksaan, yaitu dengan

mengajukan kuesioner; melakukan wawancara, observasi lapangan, dan dokumentasi; melakukan evaluasi atas penerapan pengendalian aplikasi tersebut. Langkah terakhir dari penelitian ini adalah pelaporan hasil pemeriksaan dimana peneliti akan menjabarkan temuan audit, memberikan rekomendasi dan saran-saran perbaikan, serta menyimpulkan hasil penelitian.

III. METODOLOGI

Metode yang digunakan peneliti untuk menemukan solusi terbaik di dalam menganalisa kasus ini yaitu metode COBIT (*Control Objectives for Information and Related Technology*) COBIT merupakan sekumpulan dokumentasi dan panduan yang mengarahkan pada *IT Governance* dan Management yang dapat membantu auditor, manajemen, dan pengguna (*user*) untuk menjembatani pemisah antara risiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis yang terjadi. COBIT dibagi dalam 4 domain utama yaitu:

- *Plan and Organise* (PO) - Mengarahkan perusahaan dalam penyampaian solusi (AI) sampai kepada penyampaian pelayanan (DS)
- *Acquire and Implement* (AI) - Memberikan solusi dan merubahnya menjadi suatu layanan
- *Deliver and Support* (DS) - Menerima solusi dan mengubahnya agar dapat digunakan untuk penggunaan akhir
- *Monitor and Evaluate* (ME) - Memantau seluruh proses untuk memastikan bahwa arah yang diberikan telah sesuai dijalankan.



Gambar 2. Domain Utama COBIT 4.1.

Untuk lebih memperjelas dan lebih mempermudah pengamatan, COBIT 4.1 memecah 4 domain tersebut menjadi 34 pokok pembahasan [2].

Tabel 1. Daftar Proses TI COBIT 4.1

Plan and Organise
PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.
Acquire and Implement
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.
Deliver and Support
DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.
Monitor and Evaluate
ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

Pada tahap pengumpulan data peneliti melakukan wawancara, penyebaran kuesioner, observasi, dan pengumpulan dokumentasi guna untuk mempelajari dan menganalisa pengendalian aplikasi yang diterapkan oleh perusahaan.

Desain kuesioner menggunakan skala Guttman sehingga akan didapat jawaban yang tegas yaitu ”Ya” dan ”Tidak”. Jawaban ”Ya” mengindikasikan penerapan pengendalian aplikasi ERP telah dilaksanakan, sedangkan

jawaban ”Tidak” mengindikasikan penerapan pengendalian aplikasi tidak dilaksanakan dengan baik yang kemudian akan dimasukkan dalam temuan akhir. Juga, peneliti melakukan observasi lapangan dan dokumentasi yang kemudian akan diuraikan sebagai hasil temuan yang nantinya akan dirangkum dalam sebuah laporan audit sistem informasi.

Pengukuran efektivitas penerapan pengendalian aplikasi dapat diketahui melalui hasil pengidentifikasian berdasarkan kriteria penilaian yang telah ditentukan ISACA yaitu *Maturity Model* [2]. Berikut kriteria-kriteria umum tiap level maturity model dapat dilihat pada Tabel 2.

Penghitungan hasil tingkat kematangan tiap-tiap domain dilakukan dengan penghitungan nilai yang paling sering muncul (modus) pada masing-masing proses TI. Akumulasi dengan cara modus ini dapat mempermudah pengambilan hasil akhir kematangan tiap domain.

Tabel 2. Kriteria *Maturity Model*

Level Maturity: 0 *Non-existent* **Status:** Tidak ada pengakuan dari kebutuhan untuk pengendalian internal. Kontrol bukan bagian dari budaya organisasi atau suatu misi. Terdapat risiko tinggi kekurangan kontrol dan insiden. **Pembentukan:** Tidak ada maksud untuk menilai kebutuhan untuk kontrol internal. Insiden ditangani pada saat mereka muncul.
Level Maturity: *1 Initial/ad hoc* **Status:** Ada beberapa pengakuan dari kebutuhan untuk pengendalian internal. Pendekatan dengan persyaratan risiko dan kontrol ad hoc tidak terorganisir, tanpa adanya komunikasi atau pemantauan. Kekurangan tidak diidentifikasi. Karyawan tidak menyadari tanggung jawab mereka. **Pembentukan:** Tidak ada kesadaran akan perlunya penilaian apa yang dibutuhkan dalam hal IT kontrol. Dilakukan hanya atas dasar ad hoc dan sebagai reaksi terhadap insiden yang signifikan.
Level Maturity: *2 Repeatable but intuitive* **Status:** Sudah terdapat kontrol namun tidak didokumentasikan. Operasi mereka tergantung pada pengetahuan dan motivasi individu. Efektivitas tidak cukup dievaluasi. Terdapat banyak kelemahan kontrol dan tidak ditangani, yang nantinya akan berdampak parah. Tindakan manajemen untuk menyelesaikan masalah kontrol tidak diprioritaskan. Karyawan mungkin tidak menyadari tanggung jawab mereka. **Pembentukan:** Penilaian kebutuhan kontrol terjadi hanya bila diperlukan untuk menentukan tingkat kematangan pada saat pengontrolan. Sebuah pendekatan lokakarya informal, yang melibatkan manajer TI dan tim yang terlibat dalam proses, digunakan untuk menentukan pendekatan yang memadai untuk pengontrolan, pemrosesan, dan untuk memotivasi rencana aksi yang telah disepakati.
Level Maturity: *3 Defined* **Status:** Sudah terdapat kontrol dan sudah didokumentasikan. Efektivitas operasi dievaluasi secara berkala dan terdapat rata-rata jumlah masalah. Namun, proses evaluasi tidak didokumentasikan. Sementara itu manajemen sudah mampu menduga masalah yang dapat timbul. Beberapa kelemahan kontrol masih ada dan dampak masih bisa parah. Karyawan menyadari Tanggung Jawab mereka untuk kontrol. **Pembentukan:** Proses TI yang penting diidentifikasi berdasarkan perubahan nilai dan risiko. Perincian analisis dilakukan untuk mengidentifikasi persyaratan kontrol dan akar penyebab kesenjangan yang mengembangkan peluang perbaikan. Selain lokakarya difasilitasi, alat-alat yang digunakan dan wawancara dilakukan untuk mendukung analisis dan memastikan bahwa pemilik proses TI memiliki dan mendorong proses penilaian dan perbaikan.

Level Maturity:

4 Managed and measurable

Status:

Sudah terdapat kontrol internal yang efektif dan mengukur risiko manajemen. Evaluasi, secara formal didokumentasikan dan kontrol sering dilakukan. Banyak kontrol otomatis yang sudah teratur dijalankan. Manajemen dapat mendeteksi masalah yang dapat terjadi tetapi tidak semua masalah secara rutin diidentifikasi. Ada konsisten tindak lanjut untuk mengatasi kelemahan kontrol.

Pembentukan:

Proses TI yang utama secara teratur didefinisikan dengan dukungan penuh dan kesepakatan dari pemilik proses bisnis yang relevan. Penilaian persyaratan kontrol didasarkan pada kebijakan dan kematangan yang sebenarnya dari proses ini, dan juga analisis menyeluruh dan terukur yang melibatkan *stakeholder* kunci. Akuntabilitas penilaian tersebut jelas dan ditegakkan. Strategi perbaikan didukung oleh kasus bisnis. Kinerja dalam mencapai hasil yang diinginkan secara konsisten dipantau. Ulasan kontrol eksternal diatur sesekali.

Level Maturity:

5 Optimised

Status:

Sebuah risiko perusahaan-dan program kontrol memberikan kontrol terus menerus yang efektif dan penanganan risiko. Pengendalian internal dan manajemen risiko yang terintegrasi dengan praktek perusahaan, didukung dengan otomatis *real-time monitoring* dengan tanggung jawab penuh untuk pemantauan pengendalian, manajemen risiko dan kepatuhan penegakan. Evaluasi kontrol berkelanjutan berdasarkan *self-assessment* dan kesenjangan serta analisis akar penyebab. Karyawan secara proaktif terlibat dalam perbaikan kontrol.

Pembentukan:

Perubahan bisnis menjadi pertimbangan utama proses TI, dan mencakup setiap kebutuhan untuk menilai kembali kemampuan proses kontrol. IT memproses secara teratur penilaian untuk mengkonfirmasi bahwa kontrol berada pada tingkat yang tepat dari kematangan untuk memenuhi kebutuhan bisnis dan mereka menganggap atribut kematangan untuk menemukan cara untuk membuat kontrol yang lebih efisien dan efektif.

IV. HASIL PENELITIAN

Variabel penelitian yang digunakan mencakup:

- *General Controls*
- *Boundary Controls*
- *Input Controls*
- *Process Controls*
- *Output Controls*
- *Database Controls*
- *Application Communication Controls*
- *Operating System Controls*

A. Pelaksanaan Audit

Sesuai dengan tahapan audit menurut Hunton [6], berikut proses pelaksanaan audit penelitian ini:

1. Ruang Lingkup

   Penelitian ini dilakukan pada PT. Erajaya Swasembada Tbk dengan kantor pusat yang berlokasi di Jl. Gedong Panjang 29 - 31 Pekojan – Tambora, Jakarta Barat. PT Erajaya Swasembada merupakan Erajaya Grup yang mendistribusikan dan meretail produk-produk komunikasi *mobile* seperti ponsel, ponsel pintar, *tablet*, kartu SIM, *voucher*, aksesoris, perangkat tambahan lainnya dan jasa. Sistem yang akan diteliti adalah sistem yang digunakan oleh perusahaan yaitu "Erajaya *Live Application Server*" versi Juli - Desember 2012.

2. Tujuan Audit

   Tujuan implementasi pengendalian TI adalah untuk meningkatkan kualitas pengendalian keamanan dan integritas data dari sistem informasi yang berjalan dalam lingkungan TI perusahaan, serta meminimalkan risiko sampai tingkat *acceptable*.

3. Siapkan Program Audit

   Dalam melaksanakan pemeriksaan terhadap pengendalian aplikasi, peneliti

merumuskan suatu program audit. Adapun program audit peneliti terlampir.

4. Mengumpulkan Bukti Audit

Pada tahapan ini peneliti melaksanakan program audit dengan mengumpulkan bukti-bukti. Teknik pengumpulan data yang digunakan adalah metode penelitian lapangan, yang dilakukan dengan cara mendatangi langsung obyek yang akan diteliti untuk memperoleh data primer. Sehubungan untuk mendapat data sekunder yang berhubungan dengan masalah yang menjadi obyek penelitian, maka peneliti melakukan hal-hal sebagai berikut:

1. Dokumentasi, upaya mendapatkan informasi, peneliti mengumpulkan data tertulis atau dokumen-dokumen dari perusahaan, yaitu bagan struktur organisasi, uraian tugas serta tanggung jawab, jenis *software* yang digunakan, *printscreen* dari *software* yang digunakan, serta dokumen lain yang berkaitan dengan penerapan sistem aplikasi ERP pada PT. Erajaya Swasembada Tbk.
2. Observasi, peneliti melakukan observasi langsung di perusahaan PT. Erajaya Swasembada Tbk yang berhubungan dengan sistem aplikasi ERP perusahaan. Pengamatan yang dilakukan adalah sebagai berikut:
    a. Analisis catatan (*record analysis*), meliputi catatan historis atau masa kini dan catatan umum atau pribadi, berupa tertulis, dalam bentuk *print-out*.
    b. Analisis kondisi fisik (*physical condition analysis*), analisis kondisi fisik dari obyek yang diteliti, menganalisa *hardware* yang digunakan oleh PT. Erajaya Swasembada Tbk.
    c. Analisis proses atau aktivitas (*process or activity analysis*), peneliti menganalisa aktivitas pelaksanaan input dan *output* yang dihasilkan serta aktivitas pengendalian aplikasi terhadap proses tersebut. Aktivitas ini menggunakan pendekatan *auditing around the computer*, suatu pendekatan dengan memperlakukan komputer sebagai *black box*. Peneliti tidak menguji langkah-langkah proses secara langsung tetapi membandingkan input dan *output* dari sistem. Diasumsikan bahwa jika input benar akan diwujudkan pada *output*, sehingga pemrosesannya juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.
3. Komunikasi dengan Wawancara dan Kuesioner. Wawancara yang dilakukan yaitu wawancara secara personal kepada pihak manajerial TI dengan Bpk Rencana Ginting (Cana), dan wawancara yang dilakukan dengan cara menyebarkan kuesioner. Pembuatan kuesioner menggunakan pendekatan COBIT 4.1. Setelah melakukan penyebaran kuisioner dilakukan *mapping* / pengidentifikasian pertanyaan tiap-tiap proses TI. Hal ini bertujuan agar informasi tiap-tiap proses TI COBIT dapat terpenuhi. Penyebaran kuesioner berjumlah 5 responden yang tersebar di divisi TI sebanyak 1 responden, divisi *Finance* sebanyak 1 responden, divisi *Sales* sebanyak 1 responden, divisi

Warehouse sebanyak 1 responden, dan divisi *Purchasing* sebanyak 1 responden, maka didapatkan jawaban yang sama untuk pertanyaan ya dan tidak, dengan komentar yang sedikit berbeda untuk setiap responden. Kuesioner memiliki 2 jenis yaitu kuesioner untuk TI dan kuesioner untuk non-TI. Kuesioner untuk TI terdiri dari 88 pertanyaan, yaitu 11 pertanyaan kuesioner pengendalian umum (*General Controls*), 17 pertanyaan pengendalian batasan (*Boundary Controls*), 12 pertanyaan pengendalian masukan (*Input Controls*), 10 pertanyaan pengendalian proses (*Process Controls*), 4 pertanyaan pengendalian keluaran (*Output Controls*), 17 pertanyaan pengendalian basisdata (*Database Controls*), 12 pertanyaan pengendalian komunikasi aplikasi (*Application Communication Controls*), dan 5 pertanyaan pengendalian sistem operasi (*Operating System Controls*). Sedangkan kuesioner untuk non-TI terdiri dari 65 pertanyaan, yaitu 8 pertanyaan kuesioner pengendalian umum (*General Controls*), 12 pertanyaan pengendalian batasan (*Boundary Controls*), 22 pertanyaan pengendalian masukan (*Input Controls*), 8 pertanyaan pengendalian proses (*Process Controls*), 14 pertanyaan pengendalian keluaran (*Output Controls*), dan 1 pertanyaan pengendalian komunikasi aplikasi (*Application Communication Controls*).

5. Kesimpulan Hasil Audit

Setelah melakukan tahap mengumpulkan bukti-bukti berupa hasil wawancara, observasi, dan kuesioner yang kemudian dievaluasi, maka dikumpulkan hasil temuan-temuan audit sebagai berikut:

- Tidak digunakan *Uninteruptable Power Supply* (UPS) yang mampu menstabilkan tegangan listrik pada tiap-tiap komputer yang ada.
- Tidak terdapat *dry-pipe automatic sprinkler* hanya terdapat tabung pemadam kebakaran.
- Tidak terdapat alat untuk menutup *hardware* dengan bahan tahan air dan udara sewaktu tidak digunakan.
- Tidak terdapat kontrol dalam hal membawa makanan dan minuman di dekat peralatan komputer.
- Tidak terdapat *Team Disaster Recovery Plan* yang bertugas menangani kerusakan oleh bencana. Tidak ada perencanaan ataupun penganggaran khusus berkenaan dengan tim pemulihan bencana.
- Tidak terdapat perubahan warna pada *interface*, jika terjadi kesalahan penginputan.
- Sistem tidak mampu mencegah atau mendeteksi kehilangan data selama pemrosesan.
- Sistem aplikasi tidak membatasi sistem umur *password*.
- Tidak ada penggabungan huruf kecil, besar, simbol, dan angka pada *password*.
- Sistem aplikasi tidak membatasi kegagalan *login* akses.
- Kesalahan yang telah terlanjur diinput tidak dapat di-*edit* / diperbaiki.
- Respon sistem aplikasi di setiap penginputan memakan waktu cukup lama.
- Tidak terdapat *log activity* pada sistem aplikasi.
- Tidak terdapat pemberian dan pengakhiran akses pengguna ke basisdata.

- Tidak terdapat kerangka kerja khusus untuk proyek TI, *monitoring* hanya dilakukan *ad hoc* oleh ketua team proyek.

6. Laporan Hasil Audit

Pemeriksaan yang telah dilakukan diberikan kepada pihak manajemen agar dapat segera mengambil tindakan yang dianggap perlu. Dengan adanya laporan audit sistem informasi, diperoleh kesempatan untuk menunjukkan kepada pihak manajemen manfaat dari audit sistem informasi bagi perusahaan dengan tujuan untuk meningkatkan efektifitas penerapan pengendalian aplikasi, yang terdiri dari pengendalian umum, pengendalian batasan, pengendalian input, pengendalian proses, pengendalian *output*, pengendalian basisdata, pengendalian komunikasi aplikasi, dan pengendalian sistem operasi. Berikut ringkasan laporan hasil audit yang berisikan dampak dan rekomendasi atas temuan yang didapat:

Dampak:

- Dengan tidak adanya UPS maka tidak memungkinkan *user* untuk menyimpan aktivitas yang telah dilakukan, yang belum tersimpan ketika listrik padam, sehingga risiko yang dihadapi adalah kehilangan data.
- Tidak adanya *dry-pipe automatic sprinkler* dimana aset sistem informasi berada akan mengakibatkan kerugian akan kebakaran semakin besar karena kebakaran tidak dapat ditangani sedini mungkin.
- Infrastruktur TI sangat sensitif terhadap air, api, debu, dan sebagainya, bila tidak terdapat alat pelindung untuk menutup *hardware* pada saat *hardware* dalam keadaan tidak digunakan oleh *user* maka risiko kerusakan *hardware* menjadi lebih besar.
- Bila tidak ada peraturan yang mengontrol pembawaan makanan dan minuman di dekat peralatan komputer, sewaktu-waktu minuman/makanan yang dibawa karyawan dapat tumpah dan mengenai infrastruktur TI, jika infrastruktur terkena air maka memungkinkan terjadinya reaksi hubungan arus pendek yang berakibat pada kerusakan komputer.
- Jika sewaktu-waktu perusahaan mengalami bencana maka kemungkinan besar perusahaan tidak dapat melindungi aset data/ informasi penting perusahaan. Risiko kehilangan data-data penting perusahaan menjadi sangat tinggi. Data-data penting kemungkinan besar tidak dapat tertolong dan dapat mengurangi tingkat keamanan pada data perusahaan.
- Bila tidak ada perubahan warna pada saat terjadi kesalahan penginputan data maka *user* tidak mengetahui adanya kesalahan pada saat penginputan, sehingga mengurangi keefektifan kerja *user*.
- Kehilangan data pada saat pemrosesan dapat berakibat terganggunya integritas data, apabila *user* lalai, maka kehilangan data mungkin saja terjadi, dan berakibat pada keakuratan laporan yang dihasilkan.
- Bila tidak ada pembatasan sistem umur *password* maka keamanan informasi yang dimiliki perusahaan menjadi sedikit berkurang karena, jika tidak menggunakan sistem umur *password* maka *password* dapat dengan mudah terbaca oleh orang lain ataupun pihak luar.
- Bila tidak ada penggabungan berbagai macam bentuk huruf dan angka pada *password* maka *password* menjadi lebih mudah terbaca. Terlebih bagi

para *hacker*, mereka dapat dengan mudah mengetahui *password* salah satu karyawan dan dapat dengan bebas mengakses informasi penting perusahaan.

- Orang lain yang tidak memiliki hak akses dapat mencoba-coba memasukan berbagai kemungkinan *password* yang dimiliki salah satu karyawan.
- Jika sistem aplikasi tidak memfasilitasi perbaikan kesalahan dalam penginputan maka dapat mengurangi efektifitas kerja karyawan dan mengurangi keakuratan laporan yang dihasilkan.
- Produktivitas dari para karyawan menjadi berkurang.
- Bila tidak ada *log activity* pada sistem, kehilangan data pada saat pemrosesan bisa saja terjadi. Pencarian data yang hilang ini menjadi lebih sulit karena tidak adanya *log activity* yang memudahkan dalam pengontrolan aktivitas kerja di sistem aplikasi.
- Kontrol terhadap pengaksesan basis data menjadi kurang karena tidak dapat mengetahui akses basisdata telah selesai atau belum oleh salah satu pengguna. Hal ini dapat mengakibatkan *deadlock* pada basisdata.
- Bila tidak ada kerangka kerja untuk proyek maka pengerjaan proyek menjadi tidak terjadwal dan tidak terencana dengan baik. Pengerjaan proyek dilakukan secara mendadak.

Rekomendasi:

- Sebaiknya tiap-tiap komputer terdapat UPS ynang mampu menstabilkan tegangan listrik, untuk mengantisipasi kehilangan data pada saat listrik padam.
- Memasang *dry-pipe automatic sprinkler* di dalam ruangan kerja, maupun di dalam ruang pusat data (ruang *server*).
- Sebaiknya setiap *hardware* diberikan alat pelindung dengan bahan yang tahan air dan udara, untuk mencegah kerusakan pada infrastruktur TI karena untuk melindungi debu atau air pada saat *hardware* tidak sedang digunakan oleh *user*.
- Terdapat peraturan yang mengatur pelarangan membawa makanan dan minuman ke daerah dekat infrastrutur TI.
- Mempersiapkan rencana pemulihan bencana serta pembentukan tim pemulihan bencana yang terlatih dan selalu siap jika sewaktu-waktu terjadi hal yang tidak diinginkan.
- Sistem aplikasi sebaiknya dilengkapi dengan fasilitas perubahan warna pada tampilan layar, sehingga memudahkan *user* untuk mengkoreksi apabila terjadi kesalahan penginputan.
- Sebaiknya sistem mampu mencegah atau mendeteksi kehilangan data selama pemrosesan, misalnya dengan fasilitas *auto recovery system*, sehingga aktivitas yang dilakukan sebelumnya dapat tersimpan di dalam *memory* sistem.
- Penambahan peraturan mengenai prosedur *password* yang mengharuskan mengganti *password* sistem aplikasi selama frekuensi yang disepakati, misal 3 bulan sekali.
- Membuat prosedur penulisan *password* yang merupakan penggabungan huruf kecil, huruf besar, angka, dan simbol.
- Menambahkan fasilitas pada sistem aplikasi yang dapat menutup secara otomatis jika penginputan *password* salah sebanyak input yang disepakati,

misal 5 kali.

- Menambahkan fasilitas edit pada bagian penginputan data atau sebelum dilakukannya pencetakan laporan.
- Meningkatkan kapabilitas internet perusahaan agar para pengguna dapat lebih cepat dalam penggunaan sistem aplikasi.
- Penambahan fitur *log activity* pada sistem aplikasi yang memudahkan dalam pengontrolan aktivitas kerja di sistem aplikasi
- Penambahan pengaturan mengenai batas pengakhiran akses pengguna ke basisdata.
- Sebaiknya terdapat pengaturan kerangka kerja khusus mengenai seluruh proyek perusahaan agar nantinya dapat dievaluasi keefektifan dari kerangka kerja proyek tersebut.

B. Hasil Penelitian

Pada COBIT 4.1 pengendalian internal untuk menilai kinerja dapat menggunakan *maturity model*. *Maturity model* merupakan dasar pengaturan dan pengontrolan untuk departemen TI pada suatu perusahaan. *Maturity model* dibuat untuk menilai kinerja proses TI yang dapat dijadikan landasan perusahaan dalam rangka perbaikan kinerja. Pengukuran ini dibagi menjadi 6 *level* yaitu *Non-Existent* (0), *Initial/ad hoc* (1), *Repeatable but Intuitive* (2), *Defined* (3), *Managed and Measurable* (4), dan *Optimized* (5). Penilaian atas audit dengan menggunakan pengukuran *maturity model* dibagi sesuai dengan domain COBIT.

Penghitungan hasil tingkat kematangan tiap-tiap domain dilakukan dengan penghitungan nilai yang paling sering muncul (modus) pada masing-masing proses TI.

Pengimplementasian proses TI *Plan and Organise* pada tingkat kematangan 4 - *Managed and measurable*, yaitu sebanyak 5 proses TI. Perusahaan mendapat 3 proses TI dengan tingkat kematangan 5 - *Optimised*, sedangkan 2 proses TI yang lain berada pada tingkat kematangan dibawah 3 - *Defined Process*.

Pengimplementasian proses TI *Acquire and Implement* pada tingkat kematangan 5 - *Optimised*, yaitu sebanyak 4 proses TI. Perusahaan mendapat 3 proses TI yang lain berada pada tingkat kematangan 4 - *Managed and measurable*.

Pengimplementasian proses TI *Deliver and Support* pada tingkat kematangan 4 - *Managed and measurable*, yaitu sebanyak 6 proses TI. Perusahaan mendapat 5 proses TI dengan tingkat kematangan 5 - *Optimised*, dan 2 proses TI dengan tingkat kematangan 3 - *Defined Process*.

Pengimplementasian proses TI *Monitor and Evaluate* pada tingkat kematangan 4 - *Managed and measurable*, yaitu sebanyak 3 proses TI. Perusahaan mendapat 1 proses TI dengan tingkat kematangan 3 - *Defined Process*.

V. SIMPULAN DAN SARAN

A. Simpulan

Penerapan proses TI *Plan and Organise* di departemen TI pada PT Erajaya Swasembada, Tbk dilakukan dengan membuat perencanaan strategi TI, membuat tata kelola beserta anggaran yang akan dikeluarkan, merumuskan *IT Goals* yang selaras dengan *Business Goals*, memiliki arsitektur yang jelas dalam mendokumentasikan tanggung jawab tiap-tiap bagian, bagian TI memiliki tanggung jawab penuh dalam pengadaan infrastruktur TI, memberikan pelatihan bagi para personil perusahaan, serta terintegrasinya informasi perusahaan. Pengimplementasian proses TI *Plan and Organise* pada tingkat kematangan *Managed and measurable* (*Level* 4).

Penerapan proses TI *Acquire and Implement* di departemen TI pada PT Erajaya Swasembada, Tbk dilakukan dengan merumuskan kebutuhan sistem bagi pengguna, bertanggung jawab menentukan kriteria pemilihan *vendor*, pemeliharaan infrastruktur TI, serta merumuskan materi pelatihan sistem aplikasi. Pengimplementasian proses TI *Acquire and Implement* pada tingkat

kematangan *Optimised* (*Level* 5).

Penerapan proses TI *Deliver and Support* di departemen TI pada PT Erajaya Swasembada, Tbk dilakukan dengan memastikan keselarasan *IT Goals* dan *Business Goals*, memiliki kontrak dengan pihak ketiga, pengontrolan kinerja sistem, mengontrol dan mengevaluasi pembiayaan, memiliki program pelatihan, sistem yang telah bersifat preventif, adanya pengaturan kerahasiaan data, dan kontrol yang ketat dalam pengaksesan informasi. Pengimplementasian proses TI *Deliver and Support* pada tingkat kematangan *Managed and measurable* (*Level* 4).

Penerapan proses TI *Monitor and Evaluate* di departemen TI pada PT Erajaya Swasembada, Tbk dilakukan dengan memonitor informasi operasional pada aplikasi, sistem, dan proses, dokumentasi pengontrolan dan evaluasi, kepatuhan terhadap peraturan dan kontrak, serta kejelasan pembagian tanggung jawab dan kepemilikan tugas. Pengimplementasian proses TI *Monitor and Evaluate* pada tingkat kematangan *Managed and measurable* (*Level* 4).

B. Saran

Sebaiknya perusahaan melakukan audit SI oleh pihak eksternal secara berkala, hal ini ditujukan untuk meningkatkan efektivitas dan efisiensi sistem informasi perusahaan.

Sebaiknya dalam melakukan audit SI disarankan untuk memilih nara sumber yang benar-benar menguasai *job desk* yang dimilikinya sehingga informasi yang didapat oleh auditor menjadi lebih akurat.

DAFTAR PUSTAKA

[1] Gondodiyoto, Sanyoto, Audit Sistem Informasi: Pendekatan COBIT. Edisi Revisi. Jakarta: Mitra Wacana Media, 2007.

[2] ISACA, CobiT 4.1. United States of America: IT Governance Institute, 2007.

[3] Cangemi, P. Michael and Singleton, Tommie, Managing The Audit Functio. Third Edition. United States: John Willey & Sons, 2003.

[4] Hall, James A, Information Technology Auditing and Assurance. United States: ACL Services Ltd, 2011.

[5] Weber, Ron, Information Systems Control and Audit. New Jersey: Prentice Hall, 1999.

[6] H. James, et al., Core Concepts of Information Technology Auditing. International Edition. New Jersey: John Wiley and Sons. Inc, 2004.