

=====

**AUDIT SISTEM INFORMASI PADA CV. TAMA JOGA RAYA
BERDASARKAN ANALISIS COBIT**

Oleh
**Kartika C. Kencana
Bambang Suryantoro
Jason**

ABSTRAK

Pengendalian internal terhadap sebuah sistem informasi merupakan hal yang penting dan bersifat strategis. Oleh karena itu pemahaman dan kesadaran akan hal ini sangat perlu diperhatikan oleh segenap pemilik serta pengguna aplikasi. Dengan pengendalian internal yang memadai maka diharapkan hal ini akan menjamin informasi yang dihasilkan memang bermutu dan sesuai dengan apa yang diharapkan. Sebagai sebuah perusahaan yang berkomitmen melakukan filosofi *Continuous Improvement* atau *Kaizen*, CV. Tama Joga Raya berencana untuk memperbaiki sistem informasi perusahaan dengan mengimplementasikan program yang bernama *SQL Trade*. maka penulis melakukan penelitian mengenai keberadaan pengendalian internal menurut *CobIT* dari masing-masing subsistem pada pengendalian umum dan pengendalian aplikasi, yaitu *boundary control*, *input control*, *process control* dan *output control*. Penelitian dalam Skripsi ini adalah kualitatif deskriptif sehingga tidak perlu menggunakan hipotesis dan statistik. Hasil penelitian pada CV. Tama Joga Raya berdasarkan CobIT adalah *Qualified*.

Kata kunci: *Audit, Sistem, Informasi, CobIT, Pengendalian Umum, Pengendalian Aplikasi*

PENDAHULUAN

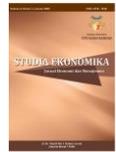
Pesatnya perkembangan peradaban manusia dewasa ini, seiring dengan penemuan dan pengembangan ilmu pengetahuan dalam bidang informasi dan komunikasi yang mampu menciptakan alat-alat yang mendukung perkembangan Teknologi Informasi, mulai dari sistem komunikasi sampai dengan alat komunikasi yang searah maupun dua arah (interaktif).

Dalam lingkungan bisnis yang begitu kompetitif dan cepat berubah, perusahaan kian menyadari manfaat potensial yang dapat dihasilkan oleh TI. Hal tersebut kemudian mendorong pihak manajemen perusahaan untuk mempertinggi ekspektasi terhadap *outcome* dan manfaat Teknologi Informasi (TI), antara lain: pengurangan waktu dalam menyampaikan layanan, peningkatan kualitas, fungsional dan kemudahan penggunaan serta perbaikan secara terus menerus yang dilakukan dengan biaya yang seminimal mungkin.

Audit sistem informasi yang berbasis pada komputerisasi membantu meningkatkan penyediaan informasi agar dapat mendukung proses pengambilan keputusan yang akan dilakukan oleh manajemen. Aktivitas yang dilakukan adalah mengembangkan sistem yang ada maupun dalam menyusun suatu sistem yang baru, serta menggantikan sistem yang lama secara keseluruhan. Perencanaan dan pengendalian operasi perusahaan senantiasa memilikisinergiuntuk terus berkembang dalam dunia bisnis.

Berdasarkan latar belakang masalah tersebut di atas, maka dirumuskan masalah sebagai berikut:

1. Apakah sistem informasi yang diterapkan oleh CV. Tama Joga Raya telah memadai?
2. Apakah terdapat kelemahan-kelemahan pada sistem informasi yang diterapkan pada CV. Tama Joga Raya?



3. Perbaikan-perbaikan apa saja yang diperlukan agar sistem informasi yang diterapkan pada CV. Tama Joga Raya dapat berjalan dengan baik?

Berdasarkan pada perumusan masalah, maka tujuan penelitian yang ingin dicapai dalam penelitian ini adalah:

1. Mengevaluasi sistem informasi yang diterapkan pada perusahaan importir dan *soledistributor* CV. Tama Joga Raya.
2. Mengidentifikasi kelemahan-kelemahan sistem informasi berdasarkan SPAP dan CobIT yang dapat terjadi di dalam aktivitas perusahaan CV. Tama Joga Raya.
3. Memberikan rekomendasi atas kelemahan sistem informasi pada CV. Tama Joga Raya.

Menurut Alvin A. Arens (2011:4): “*Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person.*” Yang berarti audit adalah pengumpulan dan evaluasi bukti mengenai informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dengan kriteria yang ditetapkan. Audit harus dilakukan oleh orang yang berkompeten dan independen.

Menurut Sekar Mayangsari dan Puspa Wandanarum (2013:7): “Auditing adalah suatu proses yang sistematis untuk memperoleh dan menilai bukti-bukti secara objektif, yang berkaitan dengan asersi-asersi tentang tindakan-tindakan dan kejadian-kejadian ekonomi untuk menentukan tingkat kesesuaian antara asersi-asersi tersebut dengan kriteria yang telah ditetapkan dan mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan.”

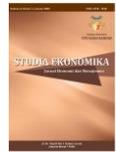
Definisi di atas mengandung arti yang luas dan berlaku untuk segala macam jenis auditing atau pengauditan yang memiliki tujuan berbeda. Adapun kalimat-kalimat kunci dalam definisi auditing di atas, menurut Sekar Mayangsari dan Puspa Wandanarum sebagai berikut:

1. Proses yang sistematis.
2. Memperoleh dan menilai bukti secara objektif.
3. Asersi-asersi tentang tindakan-tindakan dan kejadian-kejadian ekonomi.
4. Tingkat kesesuaian antara asersi-asersi dengan kriteria yang telah ditetapkan.
5. Mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan.

Jenis-jenis atau macam auditing pada dasarnya dapat dikelompokkan, serta tujuan auditing. Ditinjau dari waktu pelaksanaannya dapat dibedakan sesuai dengan pelaksanaannya, objeknya, waktu pelaksanaannya. Audit pada umumnya dibagi menjadi lima golongan menurut Sekar Mayangsari dan Puspa Wandanarum (2013:10) yaitu:

1. Ditinjau dari pelaksanaannya
 - a. Internal audit
 - b. Eksternal audit
 - c. Governmental audit
2. Ditinjau dari objek yang diaudit
 - a. Pemeriksaan laporan keuangan (*Financial Statement Audit*)
 - b. Pemeriksaan kinerja (*Management*)
 - c. Pemeriksaan kepatuhan atau kesesuaian (*Compliance Audit*)
 - d. Auditing investigasi (*Investigation Audit/Forensic Audit*)

Tujuan audit adalah untuk melakukan verifikasi bahwa subjek dari audit telah diselesaikan atau berjalan sesuai dengan standar, regulasi dan praktik yang telah disetujui dan diterima. Menurut Mulyadi tujuan dari auditing, sebagai berikut:



1. Keandalan informasi keuangan
2. Mendorong efisiensi dan efektifitas operasi
3. Pengamanan aktivita catatan
4. Kepatuhan kepada hukum dan peraturan yang berlaku

Audit dikembangkan dan dilaksanakan karena audit memberi banyak manfaat bagi dunia bisnis. Berikut manfaat-manfaat yang bisa dirasakan:

1. Penilaian Pengendalian (*Appraisal of Control*)
2. Penilaian Kinerja (*Appraisal of Performance*)
3. Membantu Manajemen (*Assistance to Management*)

Menurut Ulric J. Gelinas, JR dan Richard B.Dull:

“A system is generally consists of an integrated set of computer-based components and manual components establish to collect, store, and manage data to provide output information to users.” Yang berarti bahwa sebuah sistem pada umumnya terdiri dari suatu satuan yang terintegrasi oleh komponen komputer dan komponen *manual* untuk mungumpulkan, menyimpan, dan *me-manage* data untuk menyediakan hasil *output* berupa informasi kepada pengguna.

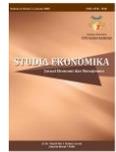
Menurut McLeod, “Informasi adalah data yang telah diproses atau data yang memiliki arti”. Dan menurut Steinburt, “Informasi adalah data yang telah diatur dan diproses untuk memberikan arti”. Jadi, informasi merupakan data yang diproses untuk memberikan arti dari data tersebut. Keuntungan informasi adalah:

1. Berkurangnya ketidakpastian (*reduction of uncertainty*)
2. Meningkatkan kualitas keputusan (*improved decision*)
3. Meningkatkan kemampuan untuk perencanaan dan menjadwalkan aktivitas (*improved ability to plan and schedule activities*)

Menurut Ron Weber, Audit SI/TI sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi asset, teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif, dengan menggunakan sumber daya secara efektif.

Menurut Standar Profesional Akuntan Publik (PSA 29 SA Seksi 508), terdapat 4 jenis pendapat akuntan, yaitu:

1. Pendapat wajar tanpa pengecualian (*Unqualified Opinion*)
Dengan pendapat wajar tanpa pengecualian, auditor menyatakan bahwa laporan keuangan menyajikan secara wajar, dalam semua hal yang material, posisi keuangan, hasil usaha, perubahan ekuitas, dan arus kas suatu entitas sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia.
2. Pendapat wajar dengan pengecualian (*Qualified Opinion*)
Pendapat wajar dengan pengecualian menyatakan bahwa laporan keuangan menyajikan secara wajar, dalam semua hal yang material, posisi keuangan, hasil usaha, perubahan ekuitas, dan arus kas sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia, kecuali untuk dampak hal yang berkaitan dengan yang dikecualikan
3. Pendapat tidak wajar (*Adverse Opinion*)
Pendapat ini dinyatakan bila, menurut pertimbangan auditor, laporan keuangan secara keseluruhan tidak disajikan secara wajar sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia
4. Pernyataan tidak memberikan pendapat (*Disclaimer Opinion*)
Auditor dapat tidak menyatakan suatu pendapat bilamana ia tidak dapat merumuskan atau tidak merumuskan suatu pendapat tentang kewajaran laporan keuangan sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia. Jika auditor menyatakan tidak memberikan pendapat, laporan



=====

auditor harus memberikan semua alasan substantive yang mendukung pertanyaan tersebut menurut Sukrisno Agoes (2012:49)

Menurut Sanyoto Gondodiyoto (2007), pengendalian internal pada sistem informasi berbasis komputer dibedakan menjadi dua, yaitu:

1. Pengendalian Umum (*General Control*)

Merupakan pengendalian akuntansi yang memiliki tujuan keamanan harta kekayaan milik perusahaan. Pengendalian ini terdiri dari:

- a. Pengendalian organisasi
- b. Pengendalian dokumentasi
- c. Pengendalian perangkat keras
- d. Pengendalian keamanan fisik
- e. Pengendalian keamanan data

2. Pengendalian Aplikasi (*Application Control*)

a. *Boundary Control* (Pengendalian Batasan) menurut Sanyoto Gondodiyoto (2007:374)

Yang dimaksud *boundary* adalah *interface* antara para pengguna (*users*) dengan sistem berbasis teknologi informasi.

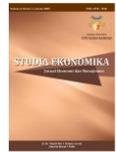
b. *Input Control* (Pengendalian Masukan) menurut Sanyoto Gondodiyoto (2007:377)

Input merupakan salah satu tahap dalam sistem komputerisasi yang paling penting dan mengandung risiko. Pengendalian masukan (*input control*) dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi yang di *input* adalah *valid*, lengkap, serta bebas dari kesalahan dan juga penyalahgunaan. *Input control* ini merupakan pengendalian aplikasi yang penting, karena *input* yang salah akan menyebabkan *output* juga keliru. Jika yang masuk sampah, maka sampah pula yang keluar (*Gold In Gold Out* atau *GIGO*). Menurut Gondodiyoto, dalam pengendalian *input* terdapat beberapa hal penting yaitu:

- *Echo Check*
- *Existence Check*
- *Matching Check*
- *Field Check*
- *Sign Check*
- *Relationship or Logical Check*
- *Limit and Reasonable Check*
- *Range Check*
- *Self-Checking Digit Check*
- *Sequence Check*
- *Label Check*
- *Zero Balance Check*
- *Numeric and Alphabetic Check*
- *Logic Check*
- *Valid Field Size Check*

c. *Process Control* (Pengendalian Proses)

Pengendalian proses (*processing control*) ialah pengendalian internal untuk mendeteksi jangan sampai data (khususnya data yang sesungguhnya sudah *valid*) menjadi *error* karena adanya kesalahan proses. Tujuan pengendalian pengolahan adalah untuk mencegah agar tidak terjadi kesalahan-kesalahan selama proses pengolahan data. Pengendalian proses ini ditujukan agar



=====

dapat mendeteksi jangan sampai terjadi data yang *error* karena terjadi salah proses. Adapun teknik-teknik yang digunakan dalam pengecekan kesalahan-kesalahan pengolahan data adalah:

- *Overflow Check*
- *Zero Balancing Check*
- Teknik *Lock out*
- *Control Total Check*
- *Matching check*
- *Reference File Check*
- *Limit and Reasonable Check*
- *Record Locking*
- *Crossfooting Check*

d. *Output Control* (Pengendalian Hasil Keluaran) menurut Sanyoto Gondodiyoto (2007:413)

Pengendalian keluaran ini dilakukan untuk menjamin agar *output* atau informasi yang disajikan adalah akurat, lengkap, mutakhir dan telah di distribusikan kepada orang-orang yang berhak. Untuk mencapai hal-hal tersebut maka digunakan beberapa metode yang cocok, diantaranya adalah

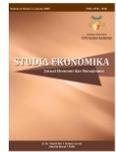
- *Preventif dalam Output Control*
Ada 2 hal penting, yaitu:
 - a) *Ouput Handling Procedures*
 - b) *Terminal Display Controls*
- *Detection dalam Output Controls*
Ada 2 hal penting, yaitu:
 - a) *Control Group Procedures*
 - b) *User Procedures*
 - c) *Corrective dalam Output Controls*
Mencakup 2 hal:
 1. *ErrorCorrection/Resubmission Procedures*
 2. *Audit Trail*

Komponen pengendalian internal yang di desain oleh COSO dikembangkan untuk diaplikasikan pada sistem berbasis *IT* yang disebut *CobIT (Control Objectives For Information and Related Technology)*. *CobIT* adalah alatpenguasaan *IT* yangmembantu dalam pemahaman danmanage risiko dan manfaat serta evaluasi yang berhubungan dengan *IT*.*CobIT* mempunyai kerangka kerja yang terdiri atas beberapa arahan (*guidelines*), menurut Riyanarto Sarno (2009:16) yakni:

1. *Control Objectives*: Terdiri atas 4 tujuan pengendalian tingkattinggi (*high level control objectives*) yang tercermin dalam 4 domain, yaitu:
 - a. Merencanakan dan Mengatur
Rencana dan Atur domain mencakup penggunaanteknologi informasi dan cara terbaik dan dapat digunakan dalam sebuah perusahaan untuk membantu perusahaan mencapai tujuan dan sasaran. Ia juga menyoroti organisasi dan infrastruktur TI adalah formulir untuk mengambil untuk mencapai hasil yang optimal dan yang palingmenghasilkan keuntungan dari penggunaan *IT*.Tabel berikut ini berisi proses TI dalam domain merencanakan dan mengatur.

Tabel1.1 Proses TI
Merencanakan dan Mengatur

PO1	Mendefinisikan rencana strategis TI
-----	-------------------------------------



PO2	Mendefinisikan arsitektur informasi
PO3	Menentukan arahan teknologi
PO4	Mendefinisikan Proses TI, organisasi dan keterhubungannya
PO5	Mengelola investasi TI
PO6	Mengkomunikasikan tujuan dan arahan manajemen
PO7	Mengelola sumber daya TI
PO8	Mengelola kualitas
PO9	Menaksir dan mengelola Resiko TI
PO10	Mengelola proyek

b. Melaksanakan dan Memperoleh

Melaksanakan dan memperoleh mencakup identifikasi persyaratan TI, memperoleh teknologi, dan menerapkan dalam proses bisnis perusahaan saat ini. Domain ini merupakan perkembangan rencana pemeliharaan bahwa perusahaan harus mengadopsi untuk memperpanjang kehidupan sebuah sistem TI dan komponennya. Tabel berikut ini berisi proses TI dalam domain melaksanakan dan memperoleh.

Tabel 1.2 Proses TI
Melaksanakan dan Memperoleh

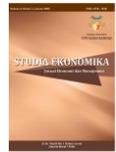
AI1	Mengidentifikasi solusi otomatis
AI2	Memperoleh dan memelihara perangkat lunak aplikasi
AI3	Memperoleh dan memelihara Infrastruktur Teknologi
AI4	Memungkinkan operasional dan penggunaan
AI5	Memenuhi sumber daya TI
AI6	Mengelola perubahan
AI7	Instalasi dan akreditasi solusi beserta perubahannya

c. Menyampaikan dan Mendukung

Dukungan yang berfokus pada domain pengiriman aspek teknologi informasi. Meliputi daerah-daerah, seperti: eksekusi aplikasi di dalam sistem TI dan hasil, serta, dukungan yang memungkinkan proses yang efektif dan efisien pelaksanaan sistem TI ini. Mendukung proses ini termasuk masalah keamanan dan pelatihan. Di bawah ini dapat dilihat mengenai tabel yang berisi proses TI dalam domain menyampaikan dan mendukung.

Tabel 1.3 Proses TI
Menyampaikan dan Mendukung

DS1	Mendefinisikan dan mengelola tingkat layanan
DS2	Mengelola layanan pihak ketiga
DS3	Mengelola kinerja dan kapasitas
DS4	Memastikan layanan yang berkelanjutan
DS5	Memastikan keamanan system
DS6	Mengidentifikasi dan mengalokasikan biaya
DS7	Mendidik dan melatih pengguna



DS8	Mengelola <i>service desk</i> dan insiden
DS9	Mengelola konfigurasi
DS10	Mengelola permasalahan
DS11	Mengelola data
DS12	Mengelola lingkungan fisik
DS13	Mengelola operasi

d. Memantau dan Evaluasi

Domain memantau dan evaluasi yang berurusan dengan strategi perusahaan dalam menilai kebutuhan perusahaan dan apakah sistem TI yang sekarang masih memenuhi tujuan yang telah dirancang dan kontrol yang diperlukan untuk mematuhi peraturan persyaratan. Pemantauan juga mencakup isu yang independen terhadap efektivitas sistem *IT* dalam kemampuan memenuhi tujuan bisnis perusahaan dan pengendalian proses oleh auditor internal dan eksternal. Tabel berikut ini berisi proses TI dalam domain memantau dan evaluasi.

Tabel 1.4 Proses TI
Memantau dan Evaluasi

ME1	Mengawasi dan mengevaluasi kinerja TI
ME2	Mengawasi dan mengevaluasi kontrol internal
ME3	Memastikan pemenuhan terhadap kebutuhan eksternal
ME4	Menyediakan Tata Kelola TI

Dalam penilaian akan domain yang ada terdapatlah teori, *IT governance maturity model* sebagai berikut:

1. Level 0 (*Non Existence*)

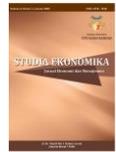
Ketika perusahaan belum menyadari kebutuhan akan keamanan TI. Tanggung jawab dan penanggung jawab belum ditentukan untuk kepastian keamanan TI tidak diimplementasikan. Tidak terdapatnya laporan keamanan TI dan tidak ada proses respon terhadap pelanggaran keamanan TI. Terdapatnya banyak kekurangan terhadap proses administrasi keamanan sistem yang ada

2. Level 1 (*Initial/ Ad Hoc*)

Saat perusahaan belum menyadari kebutuhan keamanan TI. Kesadaran akan kebutuhan keamanan terutama tergantung pada tiap individu. Keamanan TI ditempatkan berdasar pada kemampuan reaktif. Keamanan TI tidak diukur. Pelanggaran keamanan TI yang terdeteksi menyebabkan respon saling menunjuk karena tanggung jawab yang tidak jelas. Respon terhadap pelanggaran keamanan TI Tidak dapat diprediksi

3. Level 2 (*Repeatable but Intuitive*)

Ketika tanggung jawab dan penanggung jawab keamanan TI ditentukan dalam koordinator keamanan TI, walaupun manajemen otoritasnya terbatas. Kesadaran akan kebutuhan keamanan terpecah dan terbatas. Walaupun informasi terkait dengan keamanan diproduksi oleh sistem, namun tidak dianalisis. Layanan dari pihak ketiga mungkin tidak memenuhi kebutuhan keamanan perusahaan secara spesifik. Kebijakan keamanan sedang dikembangkan tetapi keahlian dan peralatan tidak mencukupi. Pelaporan keamanan TI tidak lengkap, cenderung membingungkan atau tidak berhubungan. Pelatihan keamanan tersedia namun dilakukan umumnya karena inisiatif



=====
individu. Keamanan TI terutama terlihat sebagai tanggung jawab dan area TI sementara bisnis tidak melihat keamanan TI dalam areanya

4. Level 3 (*Defined*)

Jika kesadaran akan keamanan dan dipertimbangkan oleh pihak manajemen. Prosedur keamanan TI didefinisikan dan diselarskan dengan kebijakan keamanan TI. Tanggung jawab keamanan TI ditentukan dan dipahami namun tidak diselenggarakan secara konsisten. Rencana keamanan TI dan solusi keamanan tersedia sebagai dorongan analisis risiko. Pelaporan keamanan tidak terdiri dari fokus bisnis yang jelas. Pengetesan keamanan *ad hoc* (Contoh: pengetesan gangguan) dilaksanakan. Pelatihan keamanan tersedia untuk TI dan bisnis, tetapi hanya secara informal dijadwalkan dan dikelola.

5. Level 4 (*Managed and Measurable*)

Saat tanggung jawab keamanan TI secara jelas ditentukan, dikelola dan diselenggarakan. Analisis risiko dan dampak keamanan secara konsisten dilakukan. Kebijakan dan prosedur keamanan dilengkapi dengan dasar keamanan yang spesifik. Metode untuk promosi kesadaran (*awareness*) keamanan adalah hal yang wajib. Identifikasi pengguna, otentifikasi, otorisasi distandarkan. Sertifikasi keamanan diikuti oleh anggota staf yang bertanggung jawab terhadap audit dan pengelolaan keamanan. Pengetesan keamanan dilengkapi menggunakan standard dan proses yang formal sehingga dapat meningkatkan level keamanan. Proses keamanan TI dikoordinasikan dengan fungsi keseluruhan keamanan organisasi. Pelaporan keamanan TI dikoordinasikan dengan fungsi keseluruhan keamanan organisasi. Pelaporan keamanan TI dikaitkan dengan Tujuan Bisnis. Pelatihan keamanan TI dilakukan di area bisnis dan TI. Pelatihan tersebut direncanakan dan dikelola dalam tata cara yang sesuai dengan kebutuhan bisnis dan riwayat risiko keamanan yang terdefinisi. Tujuan dan metric untuk pengelolaan keamanan sudah terdefinisi namun belum diukur

6. Level 5 (*Optimized*)

Jika keamanan TI tanggung jawab bersama dari pengelolaan bisnis dan TI serta diintegrasikan dengan tujuan bisnis keamanan perusahaan. Kebutuhan keamanan TI secara jelas terdefinisi, dioptimasi dan termasuk dalam rencana keamanan yang disetujui. Pengguna dan pelanggan secara meningkat bertanggung jawab dalam mendefinisikan kebutuhan keamanan dan fungsi keamanan terintegrasi dengan aplikasi di tahap desain. Insiden keamanan ditempatkan secara tepat dengan prosedur respon insiden formal yang didukung dengan perangkat otomatis. Penilaian keamanan periodik dilaksanakan untuk pengevaluasian efektivitas implementasi rencana keamanan. Informasi perihal *threats* dan kerentanan secara sistematis dikumpulkan dan dianalisis. Kontrol yang sistematis dikumpulkan dan dianalisis. Kontrol yang cukup untuk mitigasi risiko secara tepat dikomunikasikan dan diimplementasikan. Pengetesan keamanan, analisis penyebab dasar (*root cause analysis*) dari insiden keamanan dan identifikasi proaktif dari risiko digunakan untuk peningkatan proses yang berkelanjutan. Proses dan teknologi keamanan diintegrasikan di keseluruhan perusahaan. Metric untuk pengelolaan keamanan diukur, dikumpulkan dan dikomunikasikan. Pihak manajemen menggunakan pengukuran ini untuk membenahi rencana keamanan dalam proses perbaikan berkelanjutan.

Adapun tujuan dari CobIT ini sendiri adalah:

1. Diharapkan dapat membantu menemukan berbagai kebutuhan manajemen yang berkaitan dengan TI.
2. Agar dapat mengoptimalkan investasi TI.
3. Menyediakan ukuran atau kriteria ketika terjadi penyelewengan atau penyimpangan.

Adapun manfaat jika tujuan tersebut tercapai adalah:

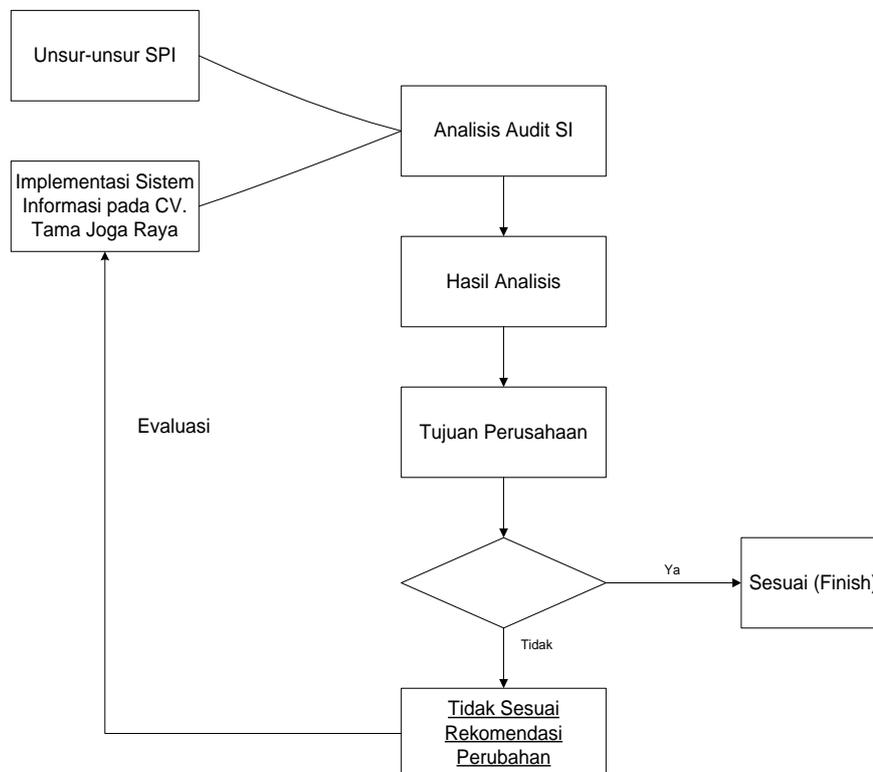
1. Dapat membantu manajemen dalam pengambilan keputusan.
2. Dapat mendukung pencapaian tujuan bisnis.
3. Dapat meminimalisasikan adanya tindak kecurangan/*fraud* yang merugikan perusahaan yang bersangkutan.

METODE

Kerangka Pikir

Kerangka pikir dari penelitian audit sistem informasi pada CV. Tama Joga Raya dapat dilihat dari gambar berikut ini:

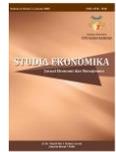
Gambar 3.1
Kerangka Pikir



Dalam penelitian ini penulis menganalisis sistem pengendalian sistem informasi yang ada pada CV. Tama Joga Raya dengan menggunakan unsur-unsur pengendalian internal dan standar CobIT sebagai dasar analisis. Hasil akhir penelitian ini berupa rekomendasi perbaikan yang diharapkan dapat meningkatkan efisiensi, efektivitas dan ekonomisasi perusahaan dalam pelaksanaan proyeknya.

Sifat dari penelitian ini adalah penelitian deskriptif, yaitu berusaha memberikan dengan sistematis dan cermat fakta-fakta aktual dan sifat populasi tertentu. Karena penelitian dalam skripsi ini adalah kualitatif deskriptif sehingga tidak perlu menggunakan hipotesis dan statistik, S. Margono(2010:36)

Variabel adalah konsep yang mempunyai nilai (misalnya tingkat pendidikan manajer). Variabel juga dapat diartikan sebagai pengelompokan yang logis dari dua atribut atau lebih. Variabel dapat dikategorikan ke dalam variabel diskrit/kategorikal dan variabel bersambung/kontinyu. Variabel



mempunyai kaitan erat dengan teori. Menurut S. Margono(2010:133)Teori adalah serangkaian konsep, definisi dan proporsi yang saling berkaitan dan bertujuan untuk memberikan gambaran yang sistematis tentang suatu fenomena.

Dalam penelitian ini variabel-variabel yang digunakan, antara lain:

1. Unsur-unsur sistem pengendalian internal.
2. Prosedur teknologi informasi/sistem informasi.
3. Implementasi Sistem Informasi pada CV. Tama Joga Raya.

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif. Penelitian kualitatif adalah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati. Sifat dari penelitian ini adalah penelitian deskriptif, yaitu berusaha memberikan dengan sistematis dan cermat fakta-fakta aktual dan sifat populasi tertentu. Karena penelitian dalam skripsi ini adalah kualitatif deskriptif sehingga tidak perlu menggunakan hipotesis dan statistik.

Dalam penelitian ini alat analisis yang digunakan adalah: *CobIT (Control Objectives for Information and related Technology)* menyediakan standar dalam kerangka kerja domain yang terdiri dari sekumpulan Proses TI yang merepresentasikan aktivitas yang dapat dikendalikan dan terstruktur.

Dalam penelitian ini penulis menggunakan data yang bersumber dari data sekunder yang bersumber primer. Data-data dalam penelitian ini dikumpulkan dengan cara :

1. Penelitian Lapangan (*Field Research*)

Dilakukan untuk memperoleh data primer dengan melakukan:

- a. Wawancara.
- b. Kuesioner.
- c. Observasi.

2. Penelitian Kepustakaan (*Library Research*)

Dilakukan untuk memperoleh data dengan meneliti dan mempelajari literatur, karya ilmiah, dan sumber-sumber bacaan lain.

HASIL PENELITIAN

Pemahaman dan Review

Sebagai perusahaan yang bergerak di dalam bidang *Automotive Refinish* dan memiliki pelanggan dalam jumlah besar, maka dibutuhkan suatu sistem atau program yang sudah terkomputerisasi guna mempercepat proses yang dijalankan perusahaan dan mempermudah pengecekan serta pemantauan data pelanggan.

Aplikasi atau program yang dipakai di dalam aktivitas perusahaan berguna untuk mengefektifkan dan mengefisienkan transaksi yang terjadi di dalam perusahaan tersebut.

Proses evaluasi terhadap sistem yang berjalan sangat diperlukan guna memperbaiki aktivitas perusahaan ke arah yang lebih baik lagi (*Kaizen/Continuous Improvement*). Dengan penerapan aplikasi atau sistem perusahaan tersebut, diharapkan dapat membantu perusahaan untuk merampingkan proses bisnis untuk meningkatkan pertumbuhan dalam berbagai hal.

Dengan memakai sistem tersebut, diharapkan perusahaan dapat memonitor semua aktivitas perusahaan dari segala sudut, sehingga bisa mendapatkan informasi yang tepat dan cepat guna membuat keputusan di dalam perusahaan. Karena modul yang ada pada sistem ini saling terintegrasi dan berkorelasi, maka dapat dilihat dalam bentuk *view* yang lengkap.

Terdiri atas 4 tujuan pengendalian tingkat tinggi (*high level control objectives*) yang tercermin dalam 4 domain, yaitu:

1. Merencanakan dan Mengatur

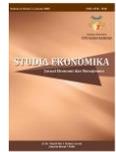
Tabel5.1Proses TI
Merencanakan dan Mengatur

Domain	Proses	Maturity Level (0-5)	Description
PO1	Mendefinisikan rencana strategis TI	2	<i>Repeatable</i>
PO2	Mendefinisikan Arsitektur Informasi	1	<i>Initial</i>
PO3	Menentukan arahan teknologi	1	<i>Initial</i>
PO4	Mendefinisikan Proses TI, organisasi dan keterhubungannya	3	<i>Defined.</i>
PO5	Mengelola investasi TI	2	<i>Repeatable</i>
PO6	Mengkomunikasikan tujuan dan arahan manajemen	1	<i>Initial</i>
PO7	Mengelola sumber daya TI	2	<i>Repeatable</i>
PO8	Mengelola kualitas	3	<i>Defined.</i>
PO9	Menaksir dan mengelola Risiko TI	2	<i>Repeatable</i>
PO10	Mengelola proyek	3	<i>Defined</i>

2. Melaksanakan dan Memperoleh

Tabel5.2 Proses TI
Melaksanakan dan Memperoleh

Domain	Proses	Maturity Level (0-5)	Description
AI1	Mengidentifikasi solusi otomatis	2	<i>Repeatable</i>
AI2	Memperoleh dan memelihara perangkat lunak aplikasi	1	<i>Initial</i>
AI3	Memproleh dan memelihara Infrastruktur Teknologi	1	<i>Initial</i>
AI4	Memungkinkan operasional dan penggunaan	2	<i>Repeatable</i>
AI5	Memenuhi sumber daya TI	1	<i>Initial</i>
AI6	Mengelola perubahan	2	<i>Repeatable</i>
AI7	Instalasi dan akreditasi solusi beserta perubahannya	2	<i>Repeatable.</i>



3. Menyampaikan dan Mendukung

Tabel5.3 Proses TI
Menyampaikan dan Mendukung

Domain	Proses	Maturity Level (0-5)	Description
DS1	Mendefinisikan dan mengelola tingkat layanan	3	<i>Defined</i>
DS2	Mengelola layanan pihak ketiga	1	<i>Initial</i>
DS3	Mengelola kinerja dan kapasitas	2	<i>Repeatable</i>
DS4	Memastikan layanan yang berkelanjutan	2	<i>Repeatable</i>
DS5	Memastikan keamanan sistem	3	<i>Defined</i>
DS6	Mengidentifikasi dan mengalokasikan biaya	2	<i>Repeatable</i>
DS7	Mendidik dan melatih pengguna	2	<i>Repeatable</i>
DS8	Mengelola <i>service desk</i> dan insiden	1	<i>Initial</i>
DS9	Mengelola konfigurasi	1	<i>Initial</i>
DS10	Mengelola permasalahan	2	<i>Repeatable</i>
DS11	Mengelola data	2	<i>Repeatable</i>
DS12	Mengelola lingkungan fisik	1	<i>Initial.</i>
DS13	Mengelola operasi	2	<i>Repeatable.</i>

4. Memantau dan Evaluasi

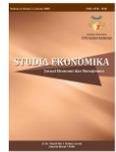
Tabel5.4 Proses TI
Memantau dan Evaluasi

Domain	Proses	Maturity Level (0-5)	Description
ME1	Mengawasi dan mengevaluasi kinerja TI	3	<i>Defined</i>
ME2	Mengawasi dan mengevaluasi kontrol internal	2	<i>Repeatable</i>
ME3	Memastikan pemenuhan terhadap kebutuhan eksternal	2	<i>Repeatable</i>
ME4	Menyediakan Tata Kelola TI	1	<i>Initial.</i>

Opini Audit

Tabel5.6Opini Audit pada Proses TI
Merencanakan dan Mengatur

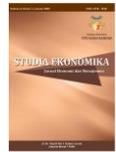
Domain	Proses	Opini	Temuan
PO1	Mendefinisikan rencana strategis TI	<i>Qualified</i>	Sudah ada penetapan rencana jangka pendek dan panjang, tetapi belum realisasi yang ada belum maksimal.



PO2	Mendefinisikan arsitektur informasi	<i>Adverse</i>	Belum ada penetapan informasi arsitektur secara tertulis.
PO3	Menentukan arahan teknologi	<i>Qualified</i>	Sudah dilakukan penentuan arah yang dilakukan, tetapi belum berjalan dengan efektif.
PO4	Mendefinisikan Proses TI, organisasi dan keterhubungannya.	<i>Unqualified</i>	Sudah dilaksanakannya korelasi atau keterkaitan antara setiap divisi di dalam proses TI berdasarkan keterkaitannya antara satu divisi ke divisi yang lain karena kebutuhan akan masing-masing divisi
PO5	Mengelola investasi TI	<i>Adverse</i>	Saat ini pengelolaan investasi TI belum dilakukan secara optimal.
PO6	Mengkomunikasikan tujuan dan arahan manajemen	<i>Qualified</i>	Sudah terdapat komunikasi tujuan dan arah manajemen yang baik, tetapi belum dilakukan pengkomunikasian secara rutin.
PO7	Mengelola sumber daya TI	<i>Adverse</i>	Saat ini telah dilakukan pengelolaan akan sumber daya TI, tetapi tidak dilakukan secara rutin, dan kerap kali akan dikelola jika terdapat masalah.
PO8	Mengelola kualitas	<i>Unqualified</i>	Sudah terdapat pengelolaan kualitas secara baik yang dilakukan oleh perusahaan. Dimana perusahaan akan berusaha semaksimal mungkin untuk meningkatkan dan mengelola kualitas yang ada.
PO9	Menaksir dan mengelola risiko TI	<i>Qualified</i>	Perusahaan telah melakukan penaksiran akan risiko TI dan mulai mencari solusi akan risiko tersebut, tetapi penaksiran dan pengelolaan risiko TI belum dilakukan secara optimal.
PO10	Mengelola proyek	<i>Unqualified</i>	Kelola proyek pada perusahaan telah berjalan dengan lancar. Karena jika terjadinya sebuah proyek, para manajer akan memfokuskan pengendalian mereka ke proyek yang ada

Tabel5.7Opini Audit pada Proses TI Melaksanakan dan Memperoleh

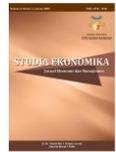
Domain	Proses	Opini	Temuan
AI1	Mengidentifikasi solusi otomatis	<i>Qualified</i>	Sudah ada identifikasi masalah secara langsung.
AI2	Memperoleh dan memelihara perangkat lunak aplikasi	<i>Adverse</i>	Terdapat kesadaran akan pemeliharaan perangkat lunak, tetapi hal tersebut seringkali diabaikan.
AI3	Memperoleh dan memelihara Infrastruktur Teknologi	<i>Adverse</i>	Tidak ada perolehan Infrastruktur Teknologi yang dilakukan secara rutin guna memelihara infrastruktur yang ada.
AI4	Memungkinkan operasional dan penggunaan	<i>Qualified</i>	Sistem yang ada pada saat ini sudah memungkinkan untuk menunjang operasional di perusahaan. Walaupun belum seutuhnya sistem tersebut bekerja secara maksimal.
AI5	Memenuhi Sumber Daya TI	<i>Adverse</i>	Saat ini sudah terdapat ide, tetapi perusahaan belum memenuhi Sumber Daya TI, karena belum ada yang mengawasi dan mengatur khusus akan TI.



AI6	Mengelola perubahan	<i>Adverse</i>	Saat ini sudah terdapat ide akan perubahan dalam TI, tetapi hal tersebut belum benar-benar di realisasikan secara umum.
AI7	Instalasi dan akreditasi solusi berdasarkan perubahannya.	<i>Qualified</i>	Sudah ada penginstalan dan akreditasi terhadap masalah tetapi belum dilakukan secara <i>continue</i> (berkelanjutan).

Tabel 5.8 Opini Audit pada Proses TI Menyampaikan dan Mendukung

Domain	Proses	Opini	Temuan
DS1	Mendefinisikan dan mengelola tingkat layanan	<i>Unqualified</i>	Hal ini sudah berjalan baik dalam proses TI.
DS2	Mengatur layanan pihak ketiga	<i>Disclaimer</i>	Saat ini pengaturan layanan akan pihak ketiga belum diterapkan.
DS3	Mengelola kinerja dan kapasitas	<i>Qualified</i>	Sudah berjalan pengelolaan kinerja dan kapasitasnya, tetapi belum dilakukan secara efektif.
DS4	Memastikan layanan yang berkelanjutan	<i>Qualified</i>	Sudah dilakukannya layanan yang berkelanjutan, tetapi belum dapat memadai, karena sistem yang ada saat ini masih terbatas.
DS5	Memastikan keamanan sistem	<i>Unqualified</i>	Keamanan sistem saat ini sudah dipastikan dengan baik. Dimana terdapat hak akses yang berbeda-beda pada setiap pemakai, berdasarkan kebutuhannya masing-masing
DS6	Mengidentifikasi dan mengalokasikan biaya	<i>Qualified</i>	Telah terdapat identifikasi dan alokasi biaya, tetapi belum dilakukan secara efektif.
DS7	Mendidik dan melatih pengguna	<i>Qualified</i>	Telah dilakukannya pelatihan dan pendidikan bagi para pengguna. Tetapi hal tersebut tidak dilakukan berkelanjutan.
DS8	Mengelola <i>service desk</i> dan insiden	<i>Adverse</i>	Saat ini pengelolaan <i>service desk</i> dan insiden hanya dilakukan jika terdapat insiden. Dalam aktivitas sehari-hari belum diberlakukan pengelolaan.
DS9	Mengatur konfigurasi	<i>Adverse</i>	Sudah terdapat pengaturan konfigurasi, tetapi hal ini jarang dilakukan dan hanya beberapa pengguna yang dapat mengatur konfigurasi.
DS10	Mengelola permasalahan	<i>Qualified</i>	Sudah berjalannya pengelolaan permasalahan tetapi belum efektif.
DS11	Mengelola data	<i>Qualified</i>	Pengelolaan data sudah berjalan secara rutin, tetapi pengelolaan tersebut belum semaksimal mungkin.
DS12	Mengelola lingkungan fisik	<i>Adverse</i>	Pengelolaan lingkungan fisik belum dilakukan secara optimal, karena belum semua dikelola dengan baik.
DS13	Mengelola operasional	<i>Qualified</i>	Pengelolaan operasional saat ini sudah berjalan, tetapi belum secara efektif dilakukan.



Tabel 5.9 Opini Audit pada Proses TI
Memantau dan Evaluasi

Domain	Proses	Opini	Temuan
ME1	Mengawasi dan mengevaluasi kinerja TI	<i>Qualified</i>	Sudah berjalan tetapi belum efektif pada aktivitas yang terjadi di dalam perusahaan. Karena terkadang kinerja TI mengalami gangguan teknis.
ME2	Mengawasi dan mengevaluasi kontrol internal	<i>Qualified</i>	Sudah terdapatnya pengawasan dan evaluasi pengendalian internal, tetapi terkadang pengendalian internal tersebut tidak berjalan dengan optimal.
ME3	Memastikan pemenuhan terhadap kebutuhan eksternal	<i>Qualified</i>	Sudah terdapat pemenuhan terhadap kebutuhan eksternal, tetapi sistem yang ada belum optimal.
ME4	Menyediakan tata kelola TI	<i>Adverse</i>	Saat ini tata kelola TI belum benar-benar dilaksanakan, baru hanya sebatas kesadaran.

Ringkasan dari keseluruhan opini audit:

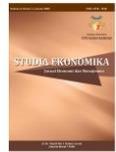
Tabel 5.10 Ringkasan Opini Audit

Opini	Total	Domain	Keterangan
<i>Unqualified</i>	5	PO4,PO8,PO10,DS1,DS5	Sudah diterapkan dan berjalan dengan baik
<i>Qualified</i>	17	PO1,PO3,PO6,PO9,AI1,AI4,AI7, DS3,DS4,DS6,DS7,DS10,DS11,DS13,ME1,ME2,ME3	Sudah diterapkan, namun masih belum optimal
<i>Adverse</i>	11	PO2,PO5,PO7,AI2,AI3,AI5,AI6, DS8,DS9,DS12,ME4	Sudah terdapat ide, tetapi hal tersebut belum benar-benar diterapkan
<i>Disclaimer</i>	1	DS2	Belum diterapkan

Jadi, dapat disimpulkan bahwa opini umum untuk CV. Tama Joga Raya adalah *Qualified*. Dimana perusahaan telah menemukan pola pengembangan yang terarah dan berjalan dengan pola yang sama, namun masih terdapat kekurangan yang masih harus dilakukan pengembangan akan sistem yang ada. Berdasarkan penilaian risiko dan pengendalian di atas maka peneliti dapat memberikan penilaian sebagai berikut :

1. Pada pengendalian manajemen keamanan memiliki penilaian risiko dan pengendalian yang diterapkan dengan standar. Dimana setiap risiko yang terjadi dapat ditanggulangi,
2. Pada pengendalian batasan memiliki penilaian risiko dan pengendalian yang standar. Ini berarti setiap risiko yang terjadi dapat ditanggulangi.
3. Pada pengendalian masukan memiliki penilaian risiko dan pengendalian yang diterapkan dengan baik.
4. Pada pengendalian proses memiliki penilaian risiko dan pengendalian yang diterapkan dengan baik.
5. Pada pengendalian keluaran memiliki nilai penilaian risiko dan pengendalian yang diterapkan adalah baik.

Secara keseluruhan kita dapat menilai bahwa pengendalian internal terhadap sistem akuntansi adalah baik. Artinya pengendalian internal yang telah diterapkan dalam perusahaan selama ini adalah sudah cukup memadai. Walaupun demikian, dengan berjalannya waktu akan terjadi perubahan oleh karena itu



perusahaan perlu melakukan evaluasi periodik guna mengakomodasi keadaan dan risiko yang mungkin terjadi. Sehingga perusahaan dapat mencegah setiap risiko yang ada, dan membuat sistem yang ada lebih efisien dan efektif.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelitian yang telah dilakukan berikut ini adalah kesimpulan dari penelitian ini adalah :

1. Sistem Informasi yang diterapkan pada perusahaan importir dan *sole* distributor CV. Tama Joga Raya secara keseluruhan sudah berjalan sesuai dengan prosedur yang telah diterapkan perusahaan. Terlebih lagi perusahaan telah menggunakan sistem SQL Tradesehingga memudahkan dan mempercepat kegiatan operasional perusahaan, namun program tersebut terkadang mengalami gangguan sistem karena terhalang akan pengembangan software tersebut. Dimana perusahaan pengembang software tersebut telah menghentikan produksi sistem tersebut.
2. Terdapat beberapa kelemahan-kelemahan sistem informasi berdasarkan SPAP dan CobIT yang dapat terjadi di dalam aktivitas perusahaan CV. Tama Joga Raya. Berdasarkan SPAP pada pengendalian aplikasi terdapat beberapa kelemahan-kelemahan yakni pada:
 - a. Pengendalian *input* yaitu *sequence check*, dimana pemeriksaan ini belum sepenuhnya diterapkan pada perusahaan. Karena terkadang data pada persediaan barang tidak sinkron.
 - b. Pada pengendalian proses beberapa pemeriksaan belum diterapkan sepenuhnya oleh perusahaan, yaitu pada *control total check*, *matching check* dan *record locking*. Berdasarkan CobIT, dari 34 proses TI dalam domain yang diaudit terdapat beberapa kelemahan dengan total 12 domain (11 *adverse*, 1 *disclaimer*).
3. Perusahaan masih memerlukan perbaikan-perbaikan agar sistem informasi yang diterapkan dapat berjalan dengan baik. Dimana perusahaan telah menemukan pola pengembangan yang terarah dan berjalan dengan pola yang sama, namun masih terdapat kekurangan yang harus diperbaiki dengan dilakukannya pengembangan akan sistem yang ada.

Saran

Dalam kesempatan ini penulis memiliki beberapa uraian rekomendasi atau saran yang mungkin berguna untuk meningkatkan efisiensi, efektifitas dan ekonomisasi khususnya untuk Sistem Informasi CV. Tama Joga Raya dengan memperbaiki kelemahan-kelemahan yang saat ini masih ada dalam pelaksanaan operasional sistem informasi, antara lain sebagai berikut:

1. Dari hasil penelitian maupun evaluasi yang telah dilakukan menunjukkan fakta bahwa sistem informasi yang diterapkan oleh perusahaan, sebaiknya terdapat perbaikan ataupun pengembangan sistem informasi yang telah diterapkan saat ini, guna meningkatkan pertumbuhan sistem informasi di masa yang akan datang. Dimana, perusahaan sebaiknya mengganti sistem TI yang saat ini dijalankan (*SQL Trade*) dengan sistem baru yang akan lebih memudahkan, mempercepat kegiatan operasional perusahaan dan tidak lupa untuk melihat tiga aspek penting lainnya, yaitu: efisien, efektif dan ekonomisasi.
2. Dengan mengidentifikasi kelemahan-kelemahan pada sistem informasi, yang berdasarkan SPAP dan CobIT. Perusahaan harus terus menerus mengimplementasikan proses perbaikan sistem informasi agar menghasilkan kinerja sistem informasi yang lebih efektif dan efisien dan mencapai tujuan perusahaan itu sendiri. Salah satunya dengan merancang peraturan-peraturan akan pengendalian aplikasi yang sudah baku sehingga setiap pengendalian dapat diterapkan dalam perusahaan, dan akan memperkecil kemungkinan akan kesalahan yang diperbuat. Dari hasil penelitian ini menunjukkan bahwa masih terdapat kelemahan-kelemahan sistem informasi yang



=====

didasarkan oleh SPAP dan CobIT, hal tersebut membuktikan bahwa kegiatan pengembangan dan perbaikan sistem informasi merupakan salah satu aktivitas yang harus dikerjakan oleh perusahaan.

3. Perusahaan sebaiknya melakukan perbaikan berkelanjutan pada proses TI. Dari hasil penelitian terdapat beberapa domain yang dianggap oleh auditor *Adverse* dan *Disclaimer*. Sehingga proses-proses TI yang saat ini mendapatkan opini *Adverse* dan *Disclaimer* dapat menjadi *Qualified* atau *Unqualified*. Dari opini tersebut timbul beberapa rekomendasi perbaikan sistem yang dapat dilakukan oleh perusahaan, sebagai berikut:
 - a. Pada proses Pengendalian TI, perusahaan sebaiknya lebih memperketat pengendalian akan pemakaian sistem, baik perangkat keras maupun perangkat lunak yang menunjang proses TI, dengan menggunakan *user id* dan *password* yang tidak diketahui orang lain, agar tidak terjadinya penyalahgunaan data.

Blue-print, Isi dari *blue-print* adalah Standard Operasional Prosedur pada Sistem Informasi. Penerapan *ITblue-print* tertulis sangat dianjurkan pada perusahaan yang bergerak di bidang distributor *automotive refinish* ini agar lebih efektif dan efisien.

DAFTAR PUSTAKA

- Agoes, Sukrisno, 2012 edisi IV, *Auditing: Petunjuk Pemeriksaan Akuntan oleh Akuntan Publik*, Salemba Empat, Jakarta
- Arens, Alvin A., Mark S. Beasley, 2010 edisi XIII, *Auditing and Assurance Service*, Global Edition, New Jersey : Pearson Prentice-Hall Inc.
- Gelinas, Ulric J. dan Richard B. Dull, 2008 edisi VII, *Accounting Information System*, Thomson South-Western, Canada.
- Gondodiyoto, Sanyoto, 2007, *Audit Sistem Informasi + Pendekatan CobIT*, Mitra Wacana Media, Jakarta
- Ikatan Akuntan Indonesia (IAI) Komptertemen Akuntan Publik (KAP), 2011, *Standar Profesional Akuntan Publik Per 1 Januari 2011*, Cetakan ke-1, Salemba Empat, Jakarta Jakarta, PSA 02 (SA 110).
- Margono S, 2010, *Metodologi Penelitian Pendidikan*, Renika Cipta, Jakarta
- Mayangsari, Sekar dan Puspa Wandanarum, 2013, *Auditing: Pendekatan Sektor Publik dan Privat*, Media Bangsa, Jakarta
- Sarno, Rianarto, 2009, *Audit Sistem Informasi dan Teknologi Informasi*, ITS Press, Surabaya