STUDI ATAS PENENTUAN RUANG LINGKUP PENGUJIAN SUBSTANTIF BERDASARKAN EVALUASI PENGENDALIAN UMUM DAN APLIKASI
(Kasus Siklus Penjualan Voucher Telepon Pada CV S)

Elizabeth Tiur Manurung[1], Elvira Yapi[2]
Fakultas Ekonomi, Universitas Katolik Parahyangan

Abstract

The purpose of this study is to determine the scope of substantive test in order to audit sales cycle. With using descriptive analytical method, this research come up to conclusion that the company has implemented a satisfied general control and application control. The company has applied all components that will increase control in sales cycle by using software accurate version 3, such as keeping up IT administration, developing system, segregation of IT function, secure control for safeguarding assets and on line, backup procedure. For application control, the company has applied control like validation test for input such as field check, sign check, size check,completeness check and prenumbered document has used in sales cycle. Especially for sales oreder, the cashier have to sign three copies to reach good control. Substantive test of transaction determined by the result of evaluation of General controls and application controls that resulted in satistfying controls, so then audit nature can use test of control, audit timing is interim, and the evidence extent will be smaller as possible.

Keywords: *IT Control, general control, application control, substantive test*

I. Pendahuluan

Perusahaan mengharapkan penggunaan teknologi dapat membantu proses bisnis lebih efektif dan efisien, meningkatkan produktivitas, pemrosesan data menjadi lebih cepat dan akurat, serta menghasilkan informasi yang lebih relevan. Sehingga teknologi menambah *value added* yang akan menjadi *competitive advantage* agar mampu bersaing.

Tekonologi informasi yang diterapkan dalam bidang akuntansi, digunakan untuk mencatat transaksi, menyimpannya dalam bentuk data, mentransformasikannya menjadi informasi dan menyebarkannya kepada para pemakai informasi.

Pada bidang audit, sistem informasi akuntansi berbasis komputer yang diterapkan di perusahaan, perlu dipahami oleh auditor (Arens, dkk, 2013:270). Dalam melakukan auditnya, auditor mesti menguji pengendalian intern perusahaan, apakah pengendailan intern telah berjalan dengan efektif dan memadai atau tidak.

Evaluasi sistem informasi perusahaan akan menjadi dasar menentukan ruang lingkup pengujian substantif. Informasi yang dihasilkan oleh sistem yang terintegrasi kualitasnya lebih baik (Arens,dkk, 2013:392).

Berdasarkan latar belakang di atas, pembahasan penelitian mengambil judul **"**Studi atas Penentuan Ruang Lingkup Pengujian Substantif Berdasarkan Evaluasi Pengendalian Umum dan Aplikasi" (Kasus Siklus Penjualan Pada CV S).

Rumusan Masalah

Beberapa permasalahan yang dibahas dalam penelitian ini, adalah:

1. Bagaimana hasil evaluasi pengendalian intern melalui *general controls* dan *application controls* pada siklus penjualan yang diterapkan perusahaan?
2. Bagaimana menentukan ruang lingkup pengujian substantif berdasarkan hasil pemeriksaan atas *general controls* dan *application controls* pada siklus penjualan di atas?

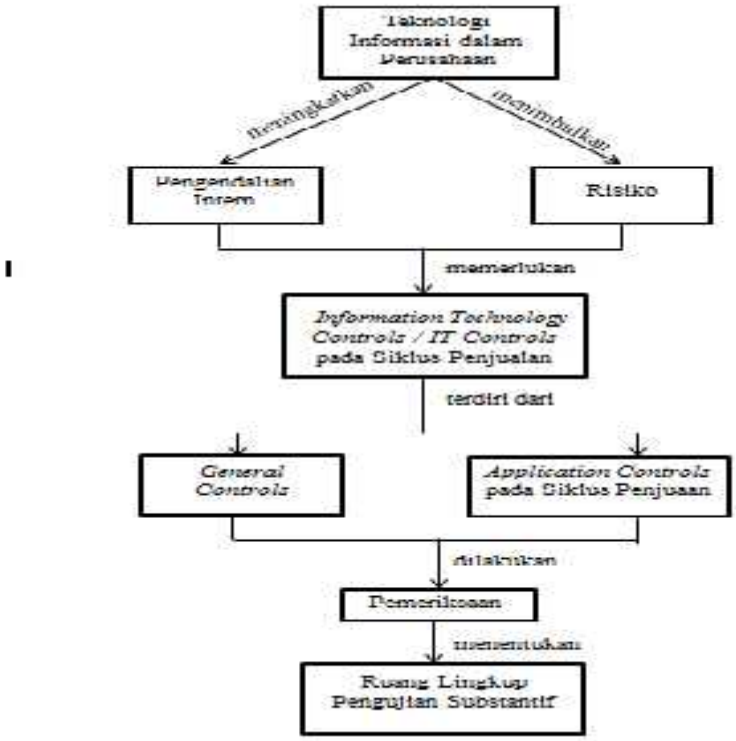
Kerangka Pemikiran

Adanya *Information technology* (IT) dalam perusahaan, diharapkan dapat meningkatkan pengendalian intern. Walaupun, penerapan teknologi informasi juga tetap menimbulkan beberapa risiko misalnya mengamankan *hardware,* atau kehilangan data, kurangnya *audit trail*, serta kebutuhan akan akhli bidang teknologi informasi.

Perusahaan perlu menambahkan pengendalian baru dalam penggunaan teknologi informasi yaitu yang disebut *IT controls*. *IT controls* terdiri dari dua, yaitu *general controls* dan *application controls*. *General controls* merupakan pengendalian untuk semua aspek fungsi teknologi informasi, Auditor mengevaluasi *general controls* untuk keseluruhan perusahaan. Sedangkan, *application controls* pengendalian pada pemrosesan transaksi. Menurut Arens,dkk, (2013:394), *application controls* akan efektif jika *general controls* juga efektif.

Sebelum melakukan pemeriksaan, auditor harus memahami *general controls* dan *application controls,* misalnya melalui observasi, wawancara dengan karyawan-karyawan yang berhubungan dengan *IT* dan melakukan pengujian terhadap sistem dokumentasi. Jika hasil pengujian atas *general controls* dan *application controls* telah memadai, maka auditor dapat mengurangi pengujian substantif dan meningkatkan pengujian terhadap pengendalian intern *(test of control)* perusahaan.

Gambar 1- Skema Kerangka Pemikiran



Landasan Teori

Audit

Audit merupakan proses mengumpulkan dan mengevaluasi bukti tentang informasi keuangan perusahaan untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dengan kriteria yang telah ditentukan sebelumnya. Audit harus dilakukan oleh pihak yang kompeten dan independen (Arens,dkk, 2013: 24).

Bukti Audit

Bukti audit adalah segala informasi yang digunakan oleh auditor untuk menentukan apakah informasi yang diaudit sesuai dengan kriteria yang telah ditetapkan (Arens,dkk, 2013:24). Menurut Arens,dkk (2013:196), terdapat dua faktor dalam *persuasiveness of evidence* yaitu *appropriate* dan *sufficient*. *Appropriateness of evidence* merupakan pengukuran atas kualitas bukti, yang berarti *relevance* dan *reliable* dalam mencapai *audit objectives* untuk *classes of transaction, account balances,* dan terkait *disclosures. Sufficiency of evidence* diukur dengan ukuran sampel yang cukup yang dipilih auditor.

Risiko Audit

Risiko audit merupakan risiko yang mana auditor gagal mengetahui salah saji laporan keuangan dalam mempersiapkan opininya (Boynton dan Raymond, 2006:352). Beberapa risiko audit menurut Arens,dkk (2013:281):

1. *Planned detection risk*
   Merupakan risiko bukti audit untuk segmen tertentu gagal mendeteksi salah saji melebihi salah saji yang ditoleransi *(tolerable misstatement)*.
2. *Inherent risk*
   Mengukur salah saji material karena *error* atau *fraud* dalam segmen sebelum mempertimbangkan efektivitas pengendalian intern.
3. *Acceptable audit risk*
   Adalah ukuran kesediaan auditor menerima kemungkinan laporan keuangan terdapat salah saji material setelah audit selesai dan opini wajar tanpa pengecualian telah diterbitkan.
4. *Control risk*
   Mengukur penilaian auditor apakah salah saji melebihi jumlah yang dapat ditolerir dalam segmen yang akan dicegah atau dideteksi secara tepat waktu dengan pengendalian intern klien.

Pengendalian Intern

Menurut COSO *Internal Control Framework* seperti yang dikutip oleh Moeller (2007: 4), menyatakan pengendalian intern adalah proses, yang dipengaruhi oleh dewan direksi, manajemen dan anggota lain dalam organisasi, dan dirancang untuk memberikan kepastian yang layak terkait dengan pencapaian tujuan, yaitu efektivitas dan efisiensi operasi, keandalan pelaporan keuangan, serta ketaatan pada hukum dan peraturan yang berlaku.

Komponen Pengendalian Intern

Menurut *COSO's Internal Control-Integrated Framework* yang dikutip oleh Arens,dkk (2013:314), terdapat lima komponen pengendalian intern untuk mencapai tujuan pengendalian, yaitu:

1. *Control environment*
   Terdiri dari tindakan, kebijakan, dan prosedur yang menggambarkan sikap keseluruhan dari manajemen tingkat atas, direktur, dan pemilik entitas mengenai pengendalian intern dan pentingnya bagi entitas.
2. *Risk asssessment*
   Penilaian risiko atas pelaporan keuangan adalah tindakan manajemen mengidentifikasi dan menganalisis risiko yang relevan dengan penyusunan laporan keuangan sesuai dengan standar yang berlaku.
3. *Control activities*
   Adalah kebijakan dan prosedur, selain yang termasuk dalam empat komponen pengendalian lainnya, yang memastikan bahwa tindakan yang dibutuhkan diambil untuk mengatasi risiko terhadap pencapaian tujuan entitas.

Menurut Hall (2011:20), *control activities* dikelompokkan menjadi dua kategori yaitu *IT controls* dan *physical controls*. *Physical controls* dibagi menjadi enam kategori yaitu:

a. *Transaction authorization*-Tujuan dari otorisasi transaksi adalah untuk memastikan bahwa semua transaksi yang material diproses oleh sistem informasi yang *valid* dan sesuai dengan tujuan manajemen.
b. *Segregation of duties*-dilakukan untuk meminimalisasi fungsi yang tidak dapat disatukan. Pemisahan fungsi utama :
   i. *Authorization*-Menyetujui transaksi dan keputusan.
   ii. *Recording*-Menyiapkan dokumen sumber; memasukkan data ke dalam sistem *online*; memelihara jurnal, buku besar, *files* atau *databases*; menyiapkan rekonsiliasi; dan menyiapkan laporan kinerja.
   iii. *Custody*-Mengatur kas, peralatan, persediaan, atau aset tetap; menerima *customer check* yang datang; dan menulis *check* pada buku akun perusahaan.
c. *Supervision*-Pada organisasi kecil atau area fungsi dengan karyawan yang kurang, maka manajemen harus mengkompensasi adanya pemisahan pengendalian dengan supervisi yang ketat.
d. *Accounting records*-Catatan akuntansi tradisional perusahaan terdiri dari dokumen sumber, jurnal, dan buku besar. Catatan-catatan ini menangkap aspek ekonomi transaksi dan menyediakan jejak audit peristiwa ekonomi.
e. *Access controls*-adalah memastikan hanya karyawan yang sah yang memiliki akses ke aktiva perusahaan. *Access control* memiliki peranan penting sebagai bagian dalam *safeguarding assets*.
f. *Independent verification*-Adalah pemeriksaan independen terhadap sistem akuntansi untuk mendeteksi *errors* dan *misrepresentation*.

4. *Information and communication*
   Tujuan sistem informasi dan komunikasi akuntansi adalah untuk memulai, mencatat, memroses, dan melaporkan transaksi entitas dan mempertahankan akuntabilitas aktiva yang bersangkutan.
5. *Monitoring*
   Aktivitas *monitoring* berhubungan dengan penilaian mutu pengendalian intern secara berkelanjutan atau periodik oleh manajemen untuk menentukan bahwa pengendalian itu telah beroperasi seperti yang diharapkan, dan telah dimodifikasi sesuai dengan perubahan kondisi.

IT (Information Technology) Controls

Meskipun teknologi informasi dapat meningkatkan pengendalian intern perusahaan, hal ini juga tetap menimbulkan risiko. Risiko ini dapat diatasi dengan pengendalian baru dalam perusahaan yaitu *IT controls*.

Menurut Arens, dkk(2013:394), dua kategori pengendalian dalam sistem teknologi informasi yaitu *general controls* dan *application controls*, yang akan dijelaskan berikut ini.

General Controls

General control berlaku untuk semua aspek dalam penggunaan *IT,* Arens, dkk (2013: 394-398), *general controls* meliputi enam kategori, yaitu:

1. *Administration of the IT function*-Sikap dewan direksi dan manajemen senior mengenai *IT* mempengaruhi pentingnya *IT* dalam organisasi. Dalam lingkungan yang kompleks, manajemen menetapkan komite pengendalian *IT* untuk membantu memantau kebutuhan teknologi informasi.
2. *Separation of IT duties* -Untuk merespon risiko atas penggabungan fungsi *authorization, custody,* dan *recording* dengan adanya komputer, organisasi merespon dengan pemisahan fungsi dalam *IT*. *Separation of IT duties* dapat dipisahkan menjadi:
   a. *IT management*-CIO atau manajer *IT* bertanggung jawab mengawasi fungsi *IT* untuk memastikan bahwa aktivitasnya telah dilaksanakan sesuai dengan rencana strategis *IT*.
   b. *Systems development-Systems analyst*, bertanggung jawab atas keseluruhan perancangan sistem aplikasi, mengkoordinasikan pengembangan dan perubahan ke sistem *IT* dengan karyawan *IT* yang bertanggung jawab dalam memrogram aplikasi, serta para pemakai sistem itu. Para *programmer* mengembangkan *flowchart* untuk setiap aplikasi baru, menyusun instruksi komputer, menguji program, dan mendokumentasikan hasilnya.
   c. *Operations-Computer operator* bertanggung jawab atas operasi komputer sehari-hari sesuai dengan jadwal yang ditetapkan CIO. *Librarian* bertanggung jawab atas pengendalian penggunaan program komputer, *file* transaksi serta catatan dan dokumentasi komputer lainnya. *Network administrator* juga mempengaruhi operasi IT karena bertanggung jawab atas perencanaan, implementasi, dan penyelenggaraan operasi jaringan *server* yang menghubungkan para pemakai dengan berbagai aplikasi serta *file* data.
   d. *Data control*-Karyawan *data input/output control* secara independen memverifikasi mutu *input* dan kelayakan *output.*
3. *Systems Development,* mencakup:
   a. Membeli *software* atau mengembangkan sendiri *software* tersebut (*in-house*) yang memenuhi kebutuhan organisasi.
   b. Menguji semua *software* guna memastikan bahwa *software* baru sesuai dengan *hardware* dan *software* yang ada, serta menentukan apakah *hardware* dan *software* itu dapat menangani volume transaksi yang diinginkan.
      i. *Pilot testing*-Sebuah sistem baru diimplementasikan di salah satu bagian dari organisasi ketika lokasi lain terus bergantung pada sistem lama.
      ii. *Parallel testing*-Sistem lama dan baru beroperasi secara bersamaan di semua lokasi.
4. *Physical and Online Security*

Pengendalian fisik atas komputer dan pembatasan *online* ke perangkat lunak serta terkait data, dapat mengurangi risiko atas perubahan yang tidak diotorisasi ke program dan penggunaan program serta *file* data yang tidak tepat. Pengendalian keamanan mencakup *physical controls* dan *online access controls*:

a. *Physical controls*-Pengendalian fisik peralatan komputer dimulai dengan membatasi akses ke *hardware, software*, serta *backupfile* data.
b. *Online access controls*-Akses pengendalian terhadap *user IDs* dan *password* yang tepat atas *software* dan terkait *file* data akan mengurangi kemungkinan adanya perubahan yang tidak diotorisasi. Paket perangkat lunak keamanan tambahan seperti program *firewall* dan enkripsi, juga dapat dipasang guna meningkatkan keamanan sistem.

5. *Backup and Contingency Planning*

Untuk mencegah kehilangan data selama listrik padam, digunakan generator, namun untuk kebakaran yang serius, kebanjiran, bencana alam, dan lainnya, perusahaan memerlukan *backup* dan rencana kontinjensi seperti menyimpan semua salinan perangkat lunak dan *file* data yang sangat penting atau meng-*outsourcing* perusahaan yang memiliki keahlian dalam mengamankan penyimpanan data tersebut.

6. *Hardware Controls*

Hardware control dibangun dalam peralatan komputer oleh produsen untuk mendeteksi dan melaporkan kegagalan peralatan. Auditor lebih berfokus pada bagaimana klien menangani kesalahan yang diidentifikasi oleh *hardware control*.

Application controls

Application controls dirancang untuk aplikasi *software*. Pengendalian yang dilakukan oleh komputer, disebut pengendalian otomatis *(automated controls)*. *Application controls* dibagi menjadi tiga kategori, yaitu

1. *Input Control*

Dirancang untuk memastikan bahwa informasi yang dimasukkan ke dalam komputer telah diotorisasi, akurat, dan lengkap. Menurut Romney dan Steinbart (2009: 322-323), pengendalian data sumber terdiri dari:

a. *Forms design*

Dokumen sumber dan formulir yang lain dirancang untuk memastikan bahwa *error* dan *omissions* dapat diminimalisasi. Dua pengendalian utama yaitu dengan memberikan nomor urut pada dokumen serta menggunakan *turnaround documents*.

b. *Cancellation and storage of documents*

Dokumen yang telah dimasukkan ke dalam sistem harus dibatalkan agar tidak dapat dimasukkan kembali ke dalam sistem baik secara sengaja maupun tidak sengaja.

c. *Authorization and segregration of duties*
Dokumen sumber harus disiapkan oleh karyawan yang memiliki otorisasi dan bertindak sesuai otorisasinya.

d. *Visual scanning*
Dokumen sumber harus dipindai untuk memastikan kelogisan dan kepemilikan sebelum dimasukkan ke dalam sistem.

Beberapa pengendalian *data entry* yang digunakan untuk memastikan validasi *input* (Romney dan Steinbart, 2009:323) antara lain:

a. *Field check*
Menentukan apakah karakter dalam *field* sudah sesuai dengan jenisnya.

b. *Sign check*
Menentukan apakah data di dalam *field* memiliki tanda aritmatik yang sesuai.

c. *Limit check*
Menguji jumlah numerik untuk memastikan bahwa jumlah tersebut tidak melebihi nilai yang sudah ditentukan sebelumnya.

d. *Range check*
Pengendalian ini serupa dengan *limit check,* kecuali dalam hal batas atas dan batas bawah

e. *Size check*
Memastikan bahwa *input data* akan cocok dengan *field* yang ditentukan.

f. *Completeness check*
Memastikan bahwa semua data yang diperlukan telah dimasukkan.

g. *Validity check*
Membandingkan nomor ID atau nomor akun transaksi dengan data yang ada di *master file* untuk memverifikasi bahwa akun tersebut ada.

h. *Reasonableness test*
Menentukan kelogisan dari data yang dimasukkan dan disimpan

i. *Check digit verification*
Memeriksa *check digit*, yang merupakan digit lain yang dihitung dari ID atau kode yang telah diotorisasi. Pengendalian *data input* dapat dibedakan antara *batch processing data entry controls* dan *online real-time processing.*

2. *Processing Control*
Processing control berguna untuk mencegah dan mendeteksi kesalahan ketika transaksi diproses. Pengendalian membantu mempertahankan integritas pemrosesan data, terdiri dari (Romney dan Steinbart, 2009:325):

a. *Data matching*

Dalam kasus tertentu, dua atau lebih jenis data harus disesuaikan terlebih dahulu sebelum suatu tindakan diambil.

b. *File labels*
Label *file* harus diperiksa untuk memastikan bahwa *file* tersebut benar dan telah diperbaharui.

c. *Recalculation of batch totals*
Batch total dihitung kembali pada setiap transaksi yang diproses dan dibandingkan dengan nilai sebelumnya.

d. *Cross-footing and zero-balance tests*
Membandingkan hasil setiap metode untuk memverifikasi keakuratan. Sedangkan, *zero-balance test* menerapkan logika yang sama untuk pengendalian suatu akun.

e. *Write-protection mechanisms*
Perlindungan terhadap penulisan atau penghapusan arsip data yang tidak sengaja dalam media magnetik.

f. *Database processing integrity procedures*
Sistem *database* menggunakan *administrator* data, kamus data, dan *concurrent update control* untuk memastikan integritas pemrosesan.

3. *Output Control*
Mendeteksi kesalahan setelah proses selesai daripada mencegah adanya kesalahan. *Output control* yang paling penting adalah meninjau kewajaran data oleh seseorang yang memiliki pengetahuan. Menurut Romney dan Steinbart (2009:326), *output controls* terdiri dari:

a. *User review of output*-Para *user* harus menguji kelogisan, kelengkapan, dan kecocokan sistem *output* yang mereka terima.

b. *Reconciliation procedures*-Semua transksi dan pembaharuan sistem lainnya direkonsiliasikan secara periodik untuk laporan pengendalian, laporan pembaharuan *file*, atau mekanisme pengendalian lainnya.

c. *External data reconciliation* - Total *database* harus direkonsiliasi secara periodik dengan data di luar sistem

Ruang Lingkup Pengujian Substantif

Auditor mempertimbangkan empat keputusan audit ketika menanggapi penilaian *risk of material misstatement* pada tingkat laporan keuangan dan tingkat asersi. Menurut Boynton dan Raymond (2006:247), keempat keputusan audit tersebut sebagai berikut:

1. *Staffing and supervision the audit*
Jika entitas memiliki pengendalian intern yang lemah dan adanya risiko yang tinggi bahwa manajemen mungkin menyimpang dari *control activities*, maka auditor menugaskan staf dengan tingkat pengalaman audit yang memadai. Auditor menugaskan staf dengan tingkat

pengalaman lebih tinggi untuk asersi audit yang memiliki tingkat subjektivitas atau kompleksitas yang tinggi.

2. *Nature of audit tests*
   Bila*risk of material misstatement* tinggi, auditor akan mengumpulkan bukti audit dengan *substantive test*. Sebaliknya, ketika *risk of material misstatement* rendah, Auditor melakukan *test of controls* yang lebih banyak dan substantive test yang lebih sedikit.
3. *Timing of audit tests*
   Keputusan mengenai waktu untuk audit meliputi saat *interim date* ataupun*fiscal year end*. Bila risiko pengendalian rendah, maka auditor melakukan *test of controls* pada *interim date*. Jika pengendalian intern efektif, maka *substantive test*selama *interim date* dan *year end* akan dikurangi. Jika pengendalian intern tidak efektif dan *risk of material misstatement* asersi tinggi, maka auditor akan melakukan *substantive tests* pada *balance sheet date*.
4. *Extent of audit tests*
   Ketika *risk of material misstatement* tinggi, auditor akan melakukan audit pada proporsi populasi yang lebih besar. Di sisi lain, ketika *risk of material misstatement* rendah, Auditor akan melakukan audit pada populasi yang lebih kecil.

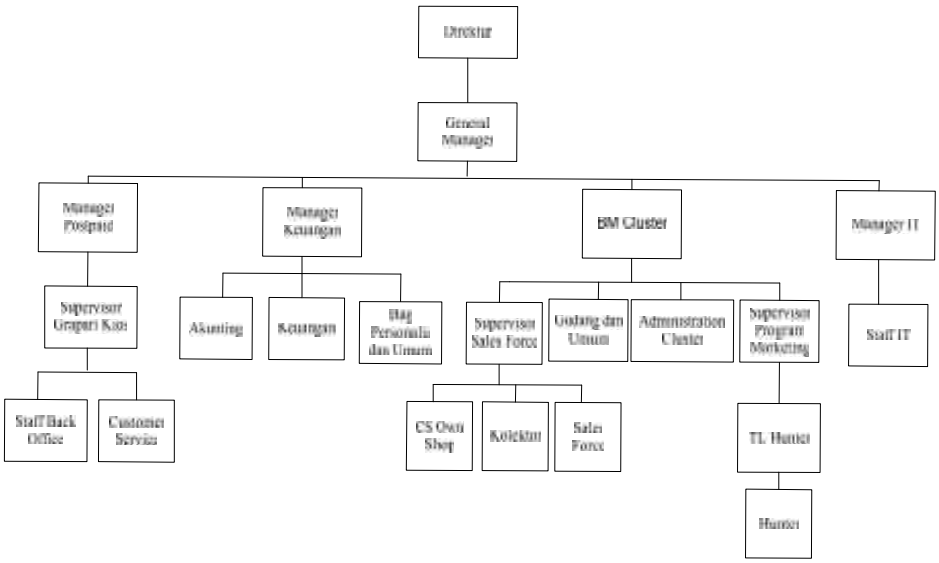
Metode dan Obyek Penelitian

Metode deskriptif analitis pada penelitian ini,dilakukan melalui pengumpulan, penganalisisan, serta menginterpretasikan data berdasarkan fakta yang ada sehingga dapat menggambarkan objek penelitian, dan dapat ditarik suatu kesimpulan.

Objek penelitian yang digunakan adalah CV S yang terletak di Jalan Veteran, Bandung. Produk yang dipasarkan adalah produk dari Telkomsel seperti perdana AS, perdana Simpati, kartu halo, *voucher* secara fisik dan elektronik. Visi yang dimiliki CV S adalah menjadi mitra Telkomsel yang dapat diandalkan dalam mengembangkan bisnis produk dan jasa Telekomunikasi, khususnya produk dari Telkomsel. Misi yang dimiliki CV S adalah memperkuat manajemen serta memperluas dan memperkuat jaringan distribusi.

Perusahaan menggunakan *software Accurate version 3* dalam menjalankan bisnisnya. *Accurate accounting software* ini merupakan sistem akuntansi yang dikembangkan untuk pencatatan dan pengelolaan keuangan perusahaan yang dibuat secara terpadu.*Software accurate version 3* ini sudah dilengkapi dengan beberapa modul seperti modul buku besar (*general ledger*), kas dan bank (*cash and bank*), persediaan (*inventory*), pembelian (*purchase*), penjualan (*sales*), dan akun tetap (*fixed asset*).

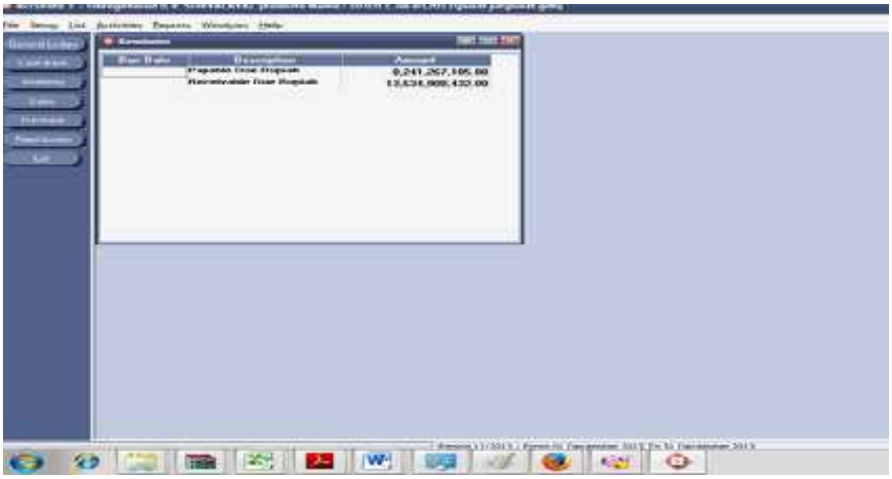
Gambar 2 - Struktur Organisasi CV Suryalaya



Hasil Penelitian

Berikut ini merupakan interface dari software Accurate version 3 yang digunakan oleh perusahaan:

Gambar 3 - *Interface* dari *Accurate Version 3*



Implementasi teknologi informasi di perusahaan didukung oleh *general controls* yang cukup memadai. Berdasarkan hasil wawancara, 65% control yang ditanyakan telah dilaksanakan, artinya terdapat kekuatan pada *general controls* perusahaan. Berikut ini merupakan rangkuman atas hasil wawancara yang dilakukan terkait dengan *general controls* perusahaan.

Tabel 1–Hasil Wawancara Pemahaman *General Controls* Perusahaan

No.	Komponen *General Control*	Ya	Tidak	Tidak Relevan

1.	Administrasi Fungsi *Information Technology*	2	4	0
2.	Pemisahan Tugas-Tugas IT	0	4	0
3.	Pengembangan Sistem	6	0	0
4.	Keamanan Fisik dan *Online*	9	4	0
5.	*Backup* dan *Contingency Planning*	3	1	0
6.	*Hardware Control*	3	0	0
Total		**23**	**13**	**0**

Sumber: Hasil Penelitian

Secara garis besar *general controls* pada perusahaan dinilai sudah efektif. Hal ini terbukti dari:

1. Perusahaan memiliki struktur organisasi formal yang mencakup bagian IT serta terdapat uraian dan tanggung jawab yang jelas dan tertulis, sehinggadapat mencegah karyawan dari penyimpangan tanggung jawab yang seharusnya dilakukan.
2. Terdapat prosedur pengembangan sistem, serta setiap perubahannya telah mendapatkan otorisasi tertulis dari pejabat yang berwenang yaitu pemilik.
3. Setiap pegawai mempunyai *user ID dan password*. Penggunaan *username* dan *password* membantu mengendalikan bahwa akses terhadap program komputer hanya dapat dilakukan oleh pihak yang memiliki wewenang.
4. Sistem *back up* terhadap *database Accurate*dilakukan setiap hari. Prosedur *backup* dapat membantu mengembalikan kondisi data apabila data tersebut secara tidak sengaja hilang, rusak, atau terhapus.
5. Setiap *username* memiliki hak akses (*access right*) tersendiri ke dalam modul-modul tertentu pada *Accurate.* Hak akses ini diberikan sesuai dengan tugas dan tanggung jawab masing-masing *user*. Terdapat pembatasan hak akses yang mengendalikan bahwa modul-modul pada *Accurate* hanya diakses oleh *user* yang memiliki wewenang.

Beberapa kelemahan *general controls* yang ditemukan dalam perusahaan, yaitu :

1. Manajemen perusahaan tidak melakukan *review* atas jadwal program kerja dan kinerja personil IT
2. Perusahaan belum melakukan program pelatihan (*training*) untuk personil IT. Hal ini disebabkan karena perusahaan hanya mempekerjakan karyawan IT yang memiliki pengetahuan dan pengalaman mengenai IT.
3. Perusahaan belum sepenuhnya melakukan pemisahan fungsi antara manajemen IT, pengembangan sistem, operasi, maupun pengendalian data.

4. Perusahaan belum memiliki kebijakan atau prosedur terkait dengan keamanan akses fisik perlengkapan komputer. Juga belum menggunakan perangkat fisik seperti gembok untuk membatasi pintu masuk ke ruang komputer.
5. Perusahaan tidak memiliki prosedur tertulis maupun lisan terkait tata cara penanganan ancaman (*disaster recovery plan*) yang berhubungan dengan sistem informasi.

Dari kelima kelemahan atas *general controls* perusahaan yang ada di atas, kelemahan nomor empat dan lima cukup signifikan. Hal ini disebabkan risiko yang dapat ditimbulkan dari kedua kelemahan tersebut berdampak besar. Kelemahan nomor empat. Meskipun perusahaan telah menggunakan CCTV untuk setiap ruangan, tidak menutup kemungkinan adanya risiko penyalahgunaan akses oleh pihak yang tidak memiliki wewenang. Risiko jika perusahaan tidak menggunakan perangkat fisik seperti gembok adalah pihak yang tidak memiliki wewenang dapat masuk sebebasnya.

Kelemahan nomor lima, diatasi hanya dengan mengandalkan sistem *back up* yang tersimpan pada *server*. Risiko yang dialami jika terjadi bencana gempa bumi yang serius, dapat mengakibatkan data hilang dan perusahaan tidak memiliki cadangan duplikasi. Walaupun terdapat dua kelemahan di atas, namun karena *control* yang lain telah berjalan dengan baik, maka *general control* dinilai cukup memadai.

Hasil pengujian *application control* juga nampak memadai. Berdasarkan hasil wawancara, 95,6% control telah dilaksanakan oleh perusahaan, artinya telah ada kekuatan pada *application controls*. Berikut ini merupakan rangkuman atas hasil wawancara terkait *application controls* pada siklus penjualan.

Tabel 2 - Pemahaman *Application Controls* Perusahaan

No.	Komponen *Application Controls*	Ya	Tidak	Tidak Relevan
1.	*Input Control*	11	1	0
2.	*Process Control*	5	0	0
3.	*Output Control*	6	0	0
Total		22	1	0

Sumber: Hasil Penelitian

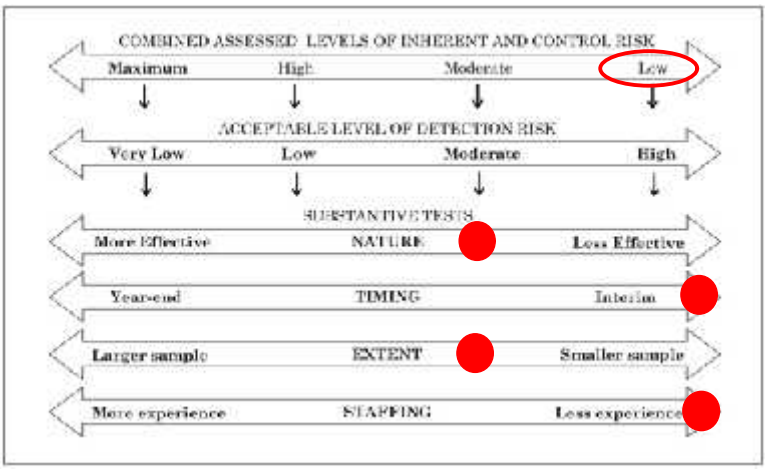
Berdasarkan hasil penelitian, *application controls* pada siklus penjualan dinilai telah memadai. Hal ini terbukti dari :

1. Sebelum melakukan penginputan *sales receipt*, bagian kasir harus menandatangani ketiga faktur tersebut. Hal ini membantu

mengendalikan bahwa transaksi yang diinput ke dalam komputer sesuai dengan fakta yang terjadi.

2. Setiap dokumen yang merupakan *input* atau *output* dari aplikasi komputer dibuat dan dirancang berdasarkan nomor urut. Pengendalian atas dokumen yang hilang dilakukan dengan baik.
3. Setiap dokumen yang telah diinput ke dalam komputer akan di cap - *cancellation*. Hal ini mencegah adanya penginputan ulang yang dilakukan karyawan.
4. Pengujian validasi berikut ini sebagai pengendalian validasi *input* seperti *field check, sign check, size check, completeness check* dan lainnya.
5. Sebelum transaksi diproses, data dicocokkan terlebih dahulu dengan data lain yang berhubungan. Adanya pencocokkan ini dapat membantu memastikan keakuratan jumlah yang diproses.
6. CV S sudah menerapkan prosedur penghancuran dokumen. Setiap dokumen yang sudah tidak terpakai dihancurkan dengan alat penghancur kertas, sehingga informasi yang ada pada laporan tidak disalahgunakan oleh pihak yang tidak memiliki wewenang

Berdasarkan hasil penelitian di atas, *general control* dan *application control* perusahaan sudah cukup memadai. Pengendalian IT pada CV S dinilai sudah diimplementasi dan dioperasikan secara memadai. Hal ini berarti kemungkinan adanya risiko salah saji menjadi kecil, sehingga menghasilkan risiko pengendalian yang rendah. Penilaian terhadap pengendalian atas *general controls* dan *application controls* ini mempengaruhi penentuan ruang lingkup pengujian substantif yaitu *nature, timing,* dan *extent* pada tahap audit. Hubungan antara *generalcontrol* dan *application control* dengan luasnya *(scope)* pemeriksaan substantif dijelaskan melalui Skema di bawah ini.



Sumber: Boynton dan Raymond (2006:247)

Skema 1 Hubungan *Control Risk* dengan *Scope substantive test of transaction*

Nature

Pengendalian IT yang memadai pada CV S menghasilkan risiko pengendalian yang rendah, maka pengujian akan lebih efektif jika memperbanyak pengujian pengendalian*(test of control).*

Timing

Pengendalian IT yang dinilai sudah memadai, sehingga risiko salah saji rendah. Sehingga pelaksanaan audit dapat dilakukan saat *interim date*.

Extent

Pengendalian IT telah memadai, menghasilkan risiko yang rendah. Artinya jumlah bukti atau sampel atas pengujian substantif menjadi lebih sedikit.

Staffing

Pada CV S, pengendalian IT telah diimplementasi secara memadai, maka auditor tidak memerlukan *IT specialist* dalam melakukan proses audit.

Kesimpulan

Berdasarkan hasil evaluasi, dapat disimpulkan bahwa *Pengendalian IT* melalui *General controls* dan *applicatin controls* pada siklus penjualan telah memadai.CV S menggunakan program aplikasi *Accurate version 3* dalam melakukan proses bisnisnya. Telah memiliki komponen*general controls* seperti administrasi fungsi IT, pemisahan tugas IT, pengembangan sistem IT, kemanan fisik dan *online*, prosedur *backup*, serta pengendalian *hardware* yang memadai. Pengembangan sistem mendapat otorisasi dari pihak berwenang dan melibatkan user sebelum sistem diimplementasikan. *Username* dan *password* juga sudah diterapkan.

Pembatasan hak akses terhadap modul *software* juga menjadi salah satu kekuatan dari *general controls* perusahaan. Telah memiliki komponen general controls seperti administrasi fungsi IT, pemisahan tugas IT, pengembangan sistem IT, kemanan fisik dan online, prosedur backup, serta pengendalian hardware yang memadai. Penentuan ruang lingkup substantif didasarkan hasil evaluasi *General controls* dan *application controls* pada siklus penjualan, yaitu sifat audit (*nature*)*,* waktu pelaksanaan audit (*timing*)*,* dan jumlah bukti (*extent*) - dapat dikurangi. *Nature* yang dipilih adalah memperbanyak pengujian pengendalian. *Timing* yang dipilih adalah saat interim. Sementara itu, jumlah bukti juga dikurangi serta tidak memerlukan IT spesialis.

Daftar Pustaka :

Arens, Alvin A., Randal J. Elder dan Marks S. Beasley. 2013. Fifteenth Edition. *Auditing and Assurance Services: An Integrated Approach*. London, UK:Pearson Education Limited.

Bodnar, George H., dan William S. Hopwood. 2001. *Accounting Information System*. Eight Edition. New Jersey: Prentice-Hall, Inc.

Boynton, William C. dan Raymond N. Johnson. 2006. Eight Edition. *Modern Auditing Assurance Services and The Integrity of Financial Reporting*. United States of America: John Wiley & Sons, Inc.

Dube, D. P., V. P. Gulati. 2005. *Information System Audit and Assurance.* New Delhi: Tata McGraw-Hill.

Gray, Iaian dan Stuart Manson. 2005. *The Audit Process : Principles, Practice, and Cases*. Third Edition. London : Thomson Learning.

Hall, James A. 2011. *Information Technology Auditing and Assurance.*Third Edition. United States of America: South-Western Cengage Learning.

Institut Akuntan Publik Indonesia. 2011. *Standar Profesional Akuntan Publik : 31 Maret 2011*. Jakarta: Salemba Empat.

Messier, Glover, dan Prawitt. 2008. *Auditing and Assurance Services : A Systematic Approach*. Sixth Edition. New York : Mc Graw-Hill.

Moeller, Robert R. 2007. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework.* USA: John Wiley & Sons, Inc.

Romney, Marshall B. dan Paul John Steinbart. 2009. Eleventh Edition. *Accounting Information Systems.* New Jersey: Pearson Education, Inc.

Sekaran, Uma dan Roger Bougie. 2010. Fifth Edition. *Research Methods For Business: A Skill Building Approach.* United Kingdom: John Wiley & Sons, Inc.

Weber, Ron. 1999. *Information Systems Control and Audit.* New Jersey: Prentice-Hall, Inc.