LAPORAN PENELITIAN

DOSEN MUDA

PERSEPSI AUDITOR INTERNAL BANK DAN AKUNTAN PENDIDIK MENGENAI EFEKTIVITAS METODE PENDETEKSIAN DAN PENCEGAHAN TINDAKAN KECURANGAN PADA SISTEM INFORMASI BERBANTUAN KOMPUTER

Oleh:

1. FEBRA ROBIYANTO, SE, MSI, AKT (KETUA)
2. DWI SUDARYATI, SE, MAcc, AKT
3. NOOR AZIS, SE, MM

Dibiayai oleh Kopertis Wilayah VI Kementrian Pendidikan Nasional
sesuai dengan Surat Perjanjian Pelaksanaan Penelitian Dosen Muda dan
Studi Kajian Wanita
Nomor: 009/006.2/SP/2010

LEMBAGA PENELITIAN
UNIVERSITAS MURIA KUDUS
2010

LAPORAN PENELITIAN

DOSEN MUDA

PERSEPSI AUDITOR INTERNAL BANK DAN AKUNTAN PENDIDIK MENGENAI EFEKTIVITAS METODE PENDETEKSIAN DAN PENCEGAHAN TINDAKAN KECURANGAN PADA SISTEM INFORMASI BERBANTUAN KOMPUTER

Oleh:

1. FEBRA ROBIYANTO, SE, MSI, AKT (KETUA)
2. DWI SUDARYATI, SE, AKT
3. NOOR AZIS, SE, MM

Dibiayai oleh Kopertis Wilayah VI Kementrian Pendidikan Nasional
sesuai dengan Surat Perjanjian Pelaksanaan Penelitian Dosen Muda dan Studi Kajian Wanita
Nomor: 009/006.2/SP/2010

LEMBAGA PENELITIAN
UNIVERSITAS MURIA KUDUS
2010

HALAMAN PENGESAHAN

1. Judul Penelitian	:	Persepsi Auditor Internal Bank dan Akuntan Pendidik mengenai Efektivitas Metode Pendeteksian dan Pencegahan Tindakan Kecurangan pada Sistem Informasi Berbantuan Komputer
2. Bidang Penelitian	:	Ekonomi
3. Ketua Peneliti		
a. Nama Lengkap	:	Febra Robiyanto, SE, MSi, Akt
b. Jenis Kelamin	:	Laki-laki
c. NIS	:	0610701000001159
d. Disiplin ilmu	:	Akuntansi
e. Pangkat/Golongan	:	Penata Muda/IIIa
f. Jabatan	:	Dosen
g. Fakultas/Jurusan	:	Ekonomi/Akuntansi
h. Alamat	:	Fak. Ekonomi UMK PO. BOX 153 Kudus
i. Telpon/Faks/E-mail	:	(0291)441643
j. Alamat Rumah	:	Jl. Bromo V/169-170 Perum. Muria Indah - Kudus
k. Telpon/Faks/E-mail	:	(0291)435282, 08156610959 febrarobiyanto@yahoo.com
4. Jumlah Anggota Peneliti	:	2 orang
a. Nama	:	Dwi Sudaryati, SE, MAcc, Akt
b. Nama	:	Noor Azis, SE, MM
5. Lokasi Penelitian	:	Jakarta, Semarang
6. Jumlah biaya	:	Rp8.500.000,00

Mengetahui,
Dekan Fakultas Ekonomi
Universitas Muria Kudus,

Drs. M. Masruri, MM
NIS. 061070201010101002

Kudus, 22 September 2010
Peneliti,

Febra Robiyanto, SE, MSi, Akt
NIS. 0610701000001159

Menyetujui
Ketua Lembaga Penelitian

Drs. H. Taufik, MS, MM
NIS. 19500411 1980031 001

ABSTRACT

This study had several purposes as follows: to find out the auditors or accountants perception of the effectiveness of fraud detection and prevention methods including used software it; to perform an empirical test on the difference in perceptions between bank internal auditors and educator accountants on the effectiveness of fraud detection and prevention methods; and to find out the most appropriate perceptions to assess the effectiveness of fraud detection and prevention method used by these auditors/acountants.

Data of the study were obtained from two sources, those from the bank internal auditors who work at top ten assets ranked general banks and those from educator accountans. The data were obtained by means of questionnaires disseminated by a survey form May 8st, 2010 to June 8th , 2010. To find out their perceptions of the effectiveness of the prevention and detection method including used software, used against the acts, the study performed analyses using Independent Sample t-test by the help of SPSS 15.0 software.

The results in auditors' knowledge on their perceptions of the effectiveness of fraud detection and prevention methods were that all methods had been adequate and reliable. They also found new methods namely Signature Verification System (SVS). Test on the hypothesis (H_A) resulted in better perceptions of the bank internal auditors than that of educator accountants of the effectiveness of fraud detection and prevention methods. According to scale used by the researchers, interval scale, in which the data were considered as preference scale, test on the hypothesis (H_A) showed the most appropriate perceptions among the two responder groups. Appropriate perceptions can be used as basic standards for selection of the most applicable perceptions to determine the effectiveness of fraud detection and prevention methods. Fraud auditing method, financial statement reconciliation, forensic accounting application in organizations, policies related to whistle blowing, data mining, protection technology using firewall and password protection were among the top ranks for the effectiveness of fraud detection and prevention methods.

Keywords: bank internal auditors' perceptions, educator accountant's perception, fraud detection methods, fraud prevention methods, and fraud of bank

ABSTRAKSI

Penelitian ini bertujuan untuk mengetahui persepsi auditor atau akuntan mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan termasuk perangkat lunak yang digunakan; menguji secara empiris perbedaan persepsi antara internal auditor bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan untuk menunjukkan persepsi yang lebih baik dari internal auditor bank; serta untuk mengetahui persepsi siapa yang paling tepat untuk mengukur ekfektivitas metode pendeteksian dan pencegahan tindakan kecurangan.

Data diperoleh dengan menyebarkan kuesioner kepada internal auditor pada sepuluh bank umum berdasarkan peringkat aset dan akuntan pendidik selama 1 bulan, dari 8 Mei 2010 sampai dengan 8 Juni 2010. Untuk mengetahui persepsi mereka mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan termasuk perangkat lunak yang digunakan, dilakukan analisis deskriptif dari pengolahan data. Selanjutnya adalah pengujian hipotesis, digunakan alat analisis *Independent Sample t Test* dengan Program *SPSS 15.0*.

Hasil pengolahan data mengenai pengetahuan auditor berkaitan dengan persepsi mereka tentang efektivitas metode pendeteksian dan pencegahan tindakan kecurangan adalah seluruh metode memiliki keefektifan lebih dari cukup dan diperoleh metode baru untuk pendeteksian dan pencegahan tindakan kecurangan dari hasil penelitian ini, yaitu teknologi untuk mendeteksi verifikasi tanda tangan dengan menggunakan *Signature Verification System* (SVS). Selanjutnya dilakukan pengujian hipotesis (H_A), terbukti bahwa persepsi internal auditor bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan. Berdasarkan skala yang digunakan, yaitu skala interval, di mana datanya merupakan skala preferensi, hasil pengujian hipotesis (H_A) dapat menunjukkan persepsi yang paling baik di antara dua kelompok responden. Persepsi yang lebih baik, dapat digunakan sebagai acuan untuk memilih persepsi siapa yang lebih tepat untuk menentukan efektivitas metode pendeteksian dan pencegahan tindakan kecurangan. Metode *fraud auditing*, rekonsiliasi laporan keuangan, penerapan akuntansi forensik di perusahaan, kebijakan yang berkaitan dengan adanya *whistle blowing*, *data mining*, teknologi perlidungan dengan metode *firewall* dan perlidungan *password* atau kata sandi; menduduki peringkat tertinggi dari efektivitas metode pendeteksian dan pencegahan tindakan kecurangan.

Kata Kunci : persepsi internal auditor bank, persepdi akuntan pendidik, metode pendeteksian *fraud*, metode pencegahan *fraud*, *fraud* bank

PRAKATA

Puji syukur ke hadirat Allah SWT, karena atas segala karunia-Nya penulis dapat menyelesaikan penelitian ini dengan lancar. Penelitian Dosen Mudadengan judul **Persepsi Auditor Internal Bank dan Akuntan Pendidik mengenai Metode Pendeteksian dan Pencegahan Tindakan Kecurangan pada Sistem Informasi Akuntansi Berbantuan Komputer** ini diajukan untuk memenuhi Tri Dharma Perguruan Tinggi.

Dalam kesempatan ini penulis bermaksud untuk mengucapkan terima kasih kepada:

1. Kopertis Wilayah VI Kementrian Pendidikan Nasional,yang telah memberi kepercayaan kepada penulis dalam melaksanakan kegiatan penelitian ini.
2. Ibu Dwi Sudaryati, SE, MAcc, Akt dan Bapak Noor Aziz, SE, MM; dengan segenap tenaga dan fikiran membantu tersusunnya laporan penelitian ini.
3. Bapak Dr. Agus Purwanto, M.Si, Ak dan Wahyu Meiranto, SE, M.Si, Ak; dan Ibu Dra. Endang Kiswara, SE, M.Si, Ak; yang banyak memberikan masukkan pada penelitian ini.
4. Istri dan Anakku tersayang, kalian yang membuatku ingin hidup seribu tahun lagi.
5. Teman-teman auditor, kalian benar-benar teman sejati.
6. Teman-teman Fakultas Ekonomi Universitas Muria Kudus, yang sangat mendukung kegiatan penelitian ini.
7. Mbak Aning dan Mbak Ardian, yang sangat membantu dalam pengumpulan data penelitian.
6. Seluruh pihak yang tidak dapat disebutkan satu persatu, atas dukungan moril ataupun materiil selama penulis menyusun tesis ini.

Penulis menyadari, dengan keterbatasan pengetahuan dan kemampuan, tentunya tesis ini banyak kekurangan. Akhirnya, semoga tesis ini dapat bermanfaat bagi masyarakat, bangsa dan negara.

Semarang, 22 September 2010
Penulis

Febra Robiyanto

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1. 1. Latar Belakang Masalah

Krisis ekonomi yang melanda Indonesia dipercaya sebagai akibat dari akumulasi tindakan kecurangan yang tidak pernah diusut tuntas. Banyak perusahaan hancur sebagai akibat kurang kuatnya pendekteksian dini terhadap tindakan kecurangan. ICW (*Indonesian Corruption Watch*), sebuah organisasi pengawas korupsi, pernah bermaksud menggugat tanggung jawab moral para auditor yang gagal menjalankan tugasnya dalam mengaudit kecurangan korporasi di Indonesia. (Parmono, 2003)

Sudah terdapat Undang-Undang untuk menjerat pelaku tindakan kecurangan, seperti Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang dapat menjerat pelaku tindakan kecurangan pada dunia maya *(cracker)* dengan pasal tindak pidana pencurian misalnya (Tuanakotta, 2007). Namun berbagai kasus tindakan kecurangan, baik oleh pihak dalam maupun luar perusahaan masih banyak terjadi. Sehingga perlu adanya metode yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan termasuk metode berbantuan komputer. Kebutuhan akan metode yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan terus berkembang seiring dengan kemajuan penggunaan teknologi informasi.

Perusahaan dengan sistem informasi berbantuan komputer sangatlah rawan akan tindakan kecurangan. Sebagai contoh: pembobolan situs web Bank Central Asia, Bank Bali dan Bank Lippo di tahun 2000, dimana salah satu pelakunya adalah seorang *cracker* Indonesia, merupakan salah satu

kegagalan pengendalian risiko dalam penggunaan teknologi informasi (Rahardjo, 2001). Kasus ini menjadi salah satu bukti bahwa teknologi yang diterapkan di perusahaan, terutama yang melakukan transaksi dengan jumlah tinggi seperti perbankan, masih kurang canggih dibandingkan dengan praktik tindakan kecurangan yang berjalan.

Pentingnya metode yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer harus mendapat perhatian dari kaum akademisi. Akuntan pendidik diharapkan memiliki pengetahuan yang memadai mengenai metode tersebut. Materi mengenai metode yang efektif ini hendaknya menjadi muatan dalam suatu mata kuliah pada Program Studi Akuntansi.

Efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer diukur melalui persepsi sesorang. Persepsi ini diambil melalui persepsi akuntan pendidik dan auditor internal bank. Akuntan pendidik dipilih karena penelitian ini diharapkan akan memberikan suatu kebijakan kepada akuntan pendidik agar memiliki pengetahuan yang memadai mengenai metode tersebut. Sedangkan auditor internal bank dipilih karena merupakan pelaku atau perancang sistem pada dunia perbankan, di mana industri perbankan merupakan industri yang telah maju dalam penggunakan sistem informasi berbantuan komputer.

Persepsi auditor internal bank dimungkinkan lebih baik dari persepsi akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan pada sistem informasi berbantuan komputer. Hal ini disebabkan karena pengalaman operasional auditor internal bank dan intensifnya pihak

perbankan sendiri dalam memperbaiki kinerja auditor internalnya demi membangun bank yang sehat.

Menanggapi masalah kerawanan atas sistem informasi berbantuan komputer, Bank Indonesia mengeluarkan Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tanggal 30 November 2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Termasuk di antaranya bank wajib memiliki kebijakan dan prosedur yang digunakan bank dalam mengelola sumber daya teknologi informasi dalam rangka mendukung kelangsungan bisnis bank terutama pelayanan kepada nasabah. Sumber daya ini mencakup antara lain perangkat keras, perangkat lunak, jaringan, sumber daya manusia serta data atau informasi. Para nasabah pastinya tidak akan memaksakan untuk menggunakan suatu layanan yang disediakan oleh pihak bank apabila mereka tidak menemukan kenyamanan dalam penggunaannya.

Standar Pelaksanaan Fungsi Audit Intern Bank (SPFAIB), wajib dilaksanakan sejak 1 Januari 1996, selanjutnya dimutakhirkan oleh Bank Indonesia dengan Peraturan Bank Indonesia No. 1/6/PBI/99 tanggal 20 September 1999. Bank wajib menyusun Piagam Audit Intern, membentuk Satuan Kerja Audit Intern (SKAI) dan menyusun panduan *audit intern*. Berkaitan dengan ini, dalam pelaksanaan fungsi *audit intern*-nya, auditor internal bank harus mempunyai:

a. Pengetahuan yang memadai dalam bidang tugasnya yaitu pengetahuan mengenai teknis audit dan disiplin ilmu lain yang relevan dengan spesialisasinya.
b. Perilaku yang independen, jujur, obyektif, tekun dan loyal.

c. Kemampuan mempertahankan kualitas profesionalnya melalui pendidikan profesi lanjutan yang berkesinambungan.
d. Kemampuan melaksanakan kemahiran profesionalnya secara cermat dan seksama.
e. Kecakapan dalam berinteraksi dan berkomunikasi baik lisan maupun tertulis secara efektif.

Kemahiran profesional dapat diperoleh auditor internal bank melalui pendidikan berkelanjutan dan pengalaman kerja yang memadai dalam bidang audit internal, kegiatan operasional perbankan serta disiplin ilmu lain yang relevan dengan spesialisasinya. Persyaratan minimal pendidikan bagi auditor internal ditetapkan oleh masing-masing bank sesuai dengan ukuran organisasi maupun tingkat kerumitan kegiatan banknya. Meskipun demikian agar dapat melaksanakan tugasnya dengan baik, latar belakang pendidikan auditor internal bank seharusnya dapat menunjang untuk:

a) memahami penerapan SPFAIB;
b) memahami standar akuntansi keuangan;
c) memahami peraturan perundang-undangan yang berkaitan dengan kegiatan operasional perbankan;
d) memahami prinsip-prinsip manajemen khususnya manajemen perbankan;
e) memiliki pengetahuan mengenai ilmu yang berkaitan dengan kegiatan perbankan seperti ilmu ekonomi, ilmu hukum, perpajakan dan masalah-masalah keuangan, metode kuantitatif/statistik serta memahami prinsip-prinsip pengolahan data elektronik.

Penelitian mengenai metode yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan termasuk metode berbantuan komputer telah dilakukan pada penelitian sebelumnya. Biestaker, *et al.* (2006) melakukan survei terhadap 86 akuntan, auditor internal dan para penyelidik akuntan bersertifikasi yang bertugas menelaah tindakan kecurangan. Penelitian ini menunjukkan ke-34 metode pendeteksian dan pencegahan tindakan kecurangan yang diteliti terbukti efektif menurut persepsi responden. Dari penelitian Biestaker ini, dikembangkan dengan membedakan persepsi antara antara akuntan pendidik dan auditor internal, informasi mengenai perangkat lunak yang digunakan pada metode berbantuan komputer serta masukkan mengenai adanya metode baru pada sistem informasi berbantuan komputer.

I.2. Perumusan Masalah

Pentingnya dilakukan penelitian mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer telah dijabarkan pada pendahuluan. Perlu dilakukan pengujian secara empiris bahwa persepsi auditor internal auditor bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Jika terbukti persepsi auditor internal bank lebih baik dari akuntan pendidik, diharapkan dapat memberikan manfaat bagi pihak akuntan pendidik. Adanya kebijakan dari pihak terkait yang mengharuskan akuntan pendidik untuk meningkatkan pengetahuan khususnya pada metode yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan pada sistem

informasi berbantuan komputer, seperti yang telah dilakukan oleh pihak perbankan. Selain itu, jika terbukti persepsi auditor internal bank lebih baik dari akuntan pendidik, dapat ditentukan persepsi yang paling tepat untuk mengukur efektivitas metode tersebut.

Berdasarkan uraian sebelumnya, rumusan masalah dalam penelitian ini adalah:

1. Perangkat lunak apa yang digunakan pada metode berbatuan komputer yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan?
2. Apakah terdapat metode berbantuan komputer yang baru yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan?
3. Apakah persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer?

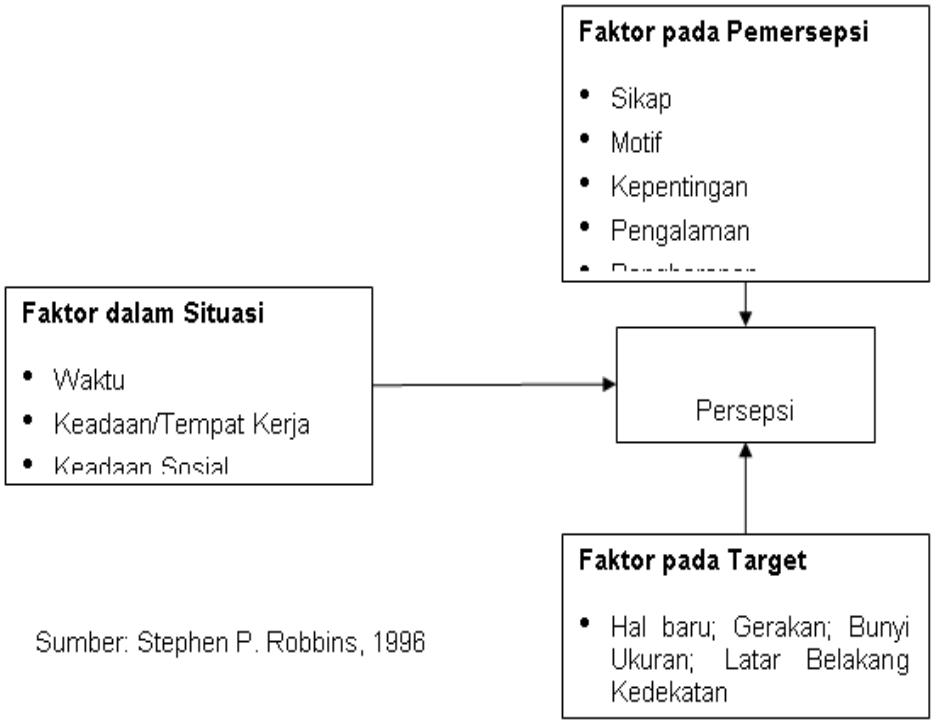
BAB II
TINJAUAN PUSTAKA

2.1. Teori Persepsi

Teori ini termasuk dalam teori psikologi individu, bahwa persepsi merupakan faktor psikologis yang mempunyai peranan penting dalam mempengaruhi perilaku seseorang. Perbedaan persepsi sangat dipengaruhi oleh interpretasi yang berbeda pada setiap individu atau kelompok. (Mahmud, 1990)

Robins (1996) secara implisit menyatakan bahwa persepsi satu individu terhadap suatu objek sangat mungkin memiliki perbedaan dengan persepsi individu yang lain terhadap obyek yang sama. Fenomena ini menurutnya dikarenakan oleh beberapa faktor yang apabila digambarkan akan tampak pada gambar 2.1.

Gambar 2.1
Faktor-faktor yang Mempengaruhi Persepsi



Sumber: Stephen P. Robbins, 1996

2.2. Tindakan Kecurangan

Tindakan kecurangan memiliki pengertian yang beragam dilihat dari berbagai perspektif, seperti deskripsi tindakan kecurangan dalam asuransi, tindakan kecurangan menurut hukum secara umum, tindakan kecurangan dalam perspektif internal auditor dan lain sebagainya. *The Institute of Internal Auditor (IIA)* di Amerika mendefinisikan tindakan kecurangan mencakup suatu kesatuan ketidakberesan *(irregularities)* dan tindakan ilegal yang bercirikan penipuan yang disengaja, dapat dilakukan oleh orang luar atau dalam organisasi. (Sawyer, 2006)

Tergantung pada siapa pelakunya, kecurangan dapat diklasifikasikan dalam dua kategori besar, yaitu (Tunggal, 1992):

1. Kecurangan untuk kepentingan perusahaan, yaitu salah saji yang timbul karena kecurangan pelaporan keuangan (*misstatements arising from fraudulent financial reporting*). Kecurangan pelaporan keuangan biasanya dilakukan karena dorongan dan ekspektasi terhadap prestasi kerja. Salah saji yang timbul karena kecurangan terhadap pelaporan keuangan umumnya dilakukan dengan sengaja, disebut dengan istilah *irregularities* (ketidakberesan). Bentuk kecurangan seperti ini seringkali dinamakan kecurangan manajamen (*management fraud*), misalnya berupa:
   - Manipulasi, pemalsuan atau pengubahan terhadap catatan akuntansi atau dokumen pendukung yang merupakan sumber penyajian laporan keuangan.

- Sengaja salah saji atau sengaja menghilangkan (*intentional omissions*) suatu transaksi, kejadian atau informasi penting dari laporan keuangan.
- Sengaja salah menerapkan prinsip-prinsip akuntansi yang berkaitan dengan jumlah, klasifikasi, penyajian atau pengungkapan di dalam laporan keuangan.

2. Kecurangan yang merugikan perusahaan yaitu salah saji yang berupa penyalahgunaan aktiva (*misstatements arising from misappropriation of assets*). Kecurangan jenis ini biasanya disebut kecurangan karyawan (*employee fraud*). Salah saji berasal dari penyalahgunaan aktiva meliputi penggelapan aktiva perusahaan yang mengakibatkan laporan keuangan tidak disajikan sesuai dengan prinsip-prinsip akuntansi yang berlaku umum. Penggelapan aktiva umumnya dilakukan oleh karyawan yang menghadapi masalah keuangan dan dilakukan karena melihat peluang kelemahan pada pengendalian internal perusahaan. Contoh salah saji jenis ini adalah:
   - Penggelapan terhadap penerimaan kas.
   - Pencurian aktiva perusahaan.
   - Penggelapan yang mengakibatkan perusahaan membayar barang dan jasa yang tidak diterima.

Albrecht (1986) menyimpulkan ada tiga elemen yang terdapat dalam tindakan kecurangan yaitu:

1. Pencurian (*theft act*), adalah pengambilan secara tidak sah uang, barang simpanan, informasi atau aset lain baik melalui cara manual, komputer atau telepon.
2. Penggelapan (*concealment*), adalah upaya penyembunyian tindakan kecurangan.
3. Konversi (*conversion*) adalah upaya mengubah aset curian menjadi hak milik sendiri dan/atau menggunakan uang hasil penjualan untuk kepentingan pribadi.

Melakukan kesalahan dengan penipuan dinamakan bermacam-macam. Ada yang menamakan *fraud, white-collar crime* (kejahatan kerah putih), penggelapan *(embezzlement)* dan lain-lain. Tindakan kecurangan *(fraud)* secara singat dinyatakan sebagai suatu penyajian yang palsu atau penyembunyian fakta yang material yang menyebabkan seseorang memiliki sesuatu. (Sawyer, 2006)

Edwin H. Sutherland pada tahun 1939 di *The American Sosiological Society Symposium* mendefinisikan tindakan kecurangan *(fraud)* sebagai *white-collar crime* (kejahatan kerah putih). Menurut Sutherland, kejahatan kerah putih adalah kejahatan yang dilakukan dalam bentuk penyalahgunaan wewenang administratif yang dimiliki seseorang. Kejahatan kerah putih diperkirakan akan semakin meningkat seiring dengan semakin berkembangnya teknologi informasi. Kemajuan teknologi informasi akan membawa dampak pada semakin cepat dan besarnya muatan data yang dapat berpindah. Mobilitas yang cepat tersebut akan mengundang pihak-pihak yang tidak bertanggung jawab untuk melakukan kecurangan terhadap

data yang ada dan menghilangkannya tanpa jejak. (Parmono, 2003)

Yang termasuk dalam kejahatan kerah putih antara lain:

1. *Embezzlement*

   Embezzlement adalah tindakan kecurangan dalam bentuk penggelapan hak milik organisasi untuk kepentingan pribadi, seperti: penggunaan kas kecil (*petty cash*) untuk kepentingan pribadi, pembuatan faktur tagihan fiktif kepada perusahaan, penggelembungan biaya perjalanan dinas, perjalanan dinas fiktif dan lain-lain.

2. *Kiting*

   Kiting adalah tindakan kecurangan dengan cara memanfaatkan transfer bank. Tindak kecurangan ini dilakukan dalam bentuk pengiriman transfer uang ke rekening sebuah institusi boneka (*dummy instituation*). Disebut sebagai institusi boneka karena institusi ini seakan-akan merupakan institusi rekanan organisasi. Padahal institusi ini hanyalah institusi rekaan yang dibuat oleh oknum dalam organisasi untuk kepentingan pribadinya. Tindakan kecurangan *kiting* bisa juga dilakukan dalam bentuk pembuatan daftar rekanan fiktif (nasabah fiktif, *supplier* fiktif), pendepositoan uang proyek terlebih dahulu untuk mendapatkan bunganya dan baru disetor kemudian pada saat akhir masa anggaran dan lain-lain.

3. *Larceny*

   Larceny adalah tindakan kecurangan yang dilakukan oleh oknum yang sebenarnya tidak memiliki otoritas atas fungsi yang dicuranginya. Bologna (1994) membedakan *larceny* dengan *embezzlement,* yaitu jika *larceny* dilakukan oleh orang yang sesungguhnya tidak memiliki otoritas atas fungsi tertentu, sedangkan *embezzlement* dilakukan oleh orang yang

memiliki otoritas atas fungsi tersebut. Contoh tindakan *larceny* antara lain: pengeluaran uang kas tanpa ijin pemilik otoritas, pembuatan cek kosong, pembuatan pembukuan ganda oleh pemegang kas, penundaan pembukuan pos penerimaan dan lain-lain.

4. *Lapping*

   Lapping adalah tindakan kecurangan dalam bentuk penyalagunaan hasil pembayaran tagihan dari pelanggan untuk kepentingan pribadi, seperti: pemakaian uang sewa suatu aset ke rekening pribadi sementara biaya operasional aset tersebut diambilkan dari anggaran rutin organisasi, komisi dari rekanan yang menerima proyek, uang hasil tagihan tidak langsung disetorkan ke organisasi tetapi disimpan dulu di rekening pribadi sampai masa penagihan selesai dan lain-lain.

5. *Pilferage*

   Pilferage adalah tindakan kecurangan dalam bentuk pencurian atau pemakaian sarana kantor dalam jumlah kecil untuk kepentingan pribadi (*petty corruption*). Tindak *pilferage* sangat sering dilakukan setiap saat dan berulang kali oleh hampir semua karyawan. Tindakan *pilferage* dilakukan seperti: pencurian atau pemakaian tidak bertanggung jawab atas alat tulis kantor (klip, kertas, pensil dan lain-lain) dalam jumlah kecil-kecil dan berulang. Tindak *pilferage* seakan sudah menjadi umum dan tidak dianggap sebagai sebuah kesalahan. Pada umumnya para pelaku selalu memiliki rasionalisasi.

2.2.1. Pihak-pihak yang Melakukan Kecurangan

Berbicara tentang kecurangan, maka bila ditilik secara mendalam

terdapat banyak sisi yang dapat dimunculkan. Di dalam jenjang hirarki perusahaan, segala tingkatan manajemen menyimpan potensi yang besar sekali untuk melakukan kecurangan mulai dari posisi *top management* sampai pada usaha yang dilakukan oleh karyawan bawahan untuk mencuri atau menggelapkan dana milik perusahaan.

Di bawah ini akan dibahas pihak-pihak yang melakukan kecurangan yaitu (Tunggal,1992) :

a. Korporasi

Kecurangan korporasi atau kejahatan ekonomi (*economic crime*) biasanya dilakukan oleh pejabat, eksekutif, manajer pusat laba (*profit center managers*) dan perusahaan publik untuk memuaskan kebutuhan ekonomis jangka pendek mereka, juga karena kerakusan ekonomi (*economic greed*) dan keserakahan/ketamakan/kekikiran (*avarice*) yang menodai nilai sosial (s*ocial values*).

b. Manajemen

Kecurangan manajemen adalah suatu bentuk kecurangan yang mempunyai arti sempit dari penggelapan, kecurangan dan pencurian. Mencakup semua bentuk penipuan yang dipraktikkan manajer untuk menguntungkan diri mereka serta merugikan perusahaan.

c. Karyawan

Kecurangan karyawan biasanya melibatkan perpindahan aktiva dari pemberi kerja. Kadang-kadang ini merupakan suatu tindakan langsung dari pencurian atau manipulasi. Pada kesempatan yang lain, terjadi dengan cara yang lain *(a roundbout way)*, seperti menaikkan pembayaran perusahaan untuk menutupi

item yang dipesan untuk penggunaan pribadi karyawan.

2.2.2. Sinyal Adanya Tindakan Kecurangan

Terdapat tanda yang bervariasi yang menunjukkan bahwa tindakan kecurangan mungkin terjadi dalam suatu perusahaan. Beberapa gejela peringatannya adalah sebagai berikut (Tunggal, 1992):

1. Laba yang dilaporkan tidak meningkat sesuai dengan harapan.

   Perusahaan mengkompilasi/mengumpulkan banyak informasi statistik yang didesain, disiapkan dan digunakan untuk menunjukkan bahwa setiap aktivitas adalah gagal apabila tidak dilaksanakan sesuai dengan harapan. Kegagalan dapat disebabkan sejumlah faktor, salah satunya adalah kecurangan karyawan.

2. Penyimpangan (*variances*) dalam barang jadi, bahan baku atau suplai.

   Apabila item dicuri, pencurian tersebut akan memunculkan suatu varian dalam perkiraan aktiva yang tepat. Kalau tidak, orang yang telah melakukan kecurangan dapat menyesuaikan catatan untuk menyembunyikan kecurangan. Apabila varian dilaporkan, daripada disembunyikan, ini mungkin menunjukkan bahwa karyawan kantor tidak terlibat dalam kecurangan. Kerugian demikian, apabila menyangkut bahan baku, suplai atau barang jadi dapat disebabkan oleh karyawan dan/atau pihak luar. Kekurangan dalam pengiriman bahan baku atau suplai akan menunjukkan suatu varian dalam laporan biaya. Laporan penerimaan barang yang palsu mungkin hasil dari ketidaktelitian atau karena tindakan konspirator (orang yang berkomplotan dalam dermaga dengan menerima renumerasi dari pengiriman). Yang perlu diingat adalah bahwa sering ada

kemungkinan bahwa penyimpangan *(variances)* disebabkan suatu kesalahan dalam standar biaya. Penyimpangan dalam barang jadi dapat diakibatkan karena kecurangan pengiriman, kesalahan dalam melaporkan mutasi atau dalam menghitung persediaan atau dari pencurian karyawan atau pihak luar. Semua kemungkinan harus dieksplorasi agar dapat mengurangi varian produk barang jadi. Kerugian yang konsisten dari produk biasanya merupakan suatu tanda pencurian.

3. Peningkatan jumlah biaya operasi yang tidak dapat dijelaskan.

   Apabila catatan menunjukkan bahwa suatu operasi mengalami peningkatan dalam biaya operasi dan menajemen lokal tidak dapat menjawabnya, memberikan indikasi akan adanya tindakan kecurangan. Kadang-kadang peningkatan biaya karena pengeluaran yang tidak normal dibebankan ke operasi tanpa pengetahuan dan persetujuan manajemen lokal. Faktor-faktor fiktif seperti biaya untuk pembelian pribadi, dapat diproses dengan dasar persetujuan yang palsu.

4. Peningkatan yang tidak dapat dijelaskan dalam biaya bahan, suplai atau upah.

   Peningkatan upah langsung yang tidak dapat dijelaskan sering merupakan hasil dari penambahan upah *(payroll padding)*. Peningkatan mungkin hasil dari pembayaran lebih karena praktik pembelian yang buruk atau adanya kolusi antara bagian pembelian dengan pemasok. Apakah seorang karyawan dalam posisi untuk mengambil keputusan, berkomplot dengan pihak luar untuk membayar harga yang telah dinaikkan *(inflated price)*. Pemasok biasanya memberi sebagian ”*kickback*” atau semua kelebihan pembayaran tersebut. Apabila curiga terhadap tawaran yang diajukan,

maka perlu mempertimbangkan penggunaan agen pihak luar untuk mempelajari kewajaran harga untuk item yang dipertanyakan.

5. Laporan tanpa nama dari transaksi yang diragukan/dipertanyakan.

Di bawah ini adalah beberapa praktik ketidakjujuran yang biasanya terjadi dan tanda peringatannya (Tunggal, 1992):

1. Menaikkan upah (*payroll padding*) atau tipe manipulasi upah yang lain.

   Tanda peringatannya (*waring padding*) adalah:

   - Kenaikkan biaya upah
   - Berkurangnya efisiensi upah.
   - Eliminasi prosedur pengendalian internal tertentu.

2. Pencurian produk.

   Tanda peringatannya adalah:

   - Kekurangan persediaan yang dilaporkan.
   - Kondisi ketiadaan persediaan yang tidak direfleksikan pada laporan status persediaan harian.
   - Kenaikan sampel, kerusakan barang (*spoil*), *scrap*, sampah atau sisa (*salvage*).
   - Tingkat yang tinggi dari penyesuaian-penyesuaian (adjustments) terhadap angka-angka persediaan.

3. Pengalihan (*diversion*) pembayaran piutang dagang.

   Tanda peringatannya adalah:

   - Terjadinya perbedaan antara kerugian piutang dengan perkiraan pengendalian (*control accounts*).

- Banyak keluhan pelanggan tentang ketidaktepatan dalam penagihan atau atas ”*statement of account*”.
- Banyak pengeluaran memo kredit.
- Banyak penyesuaian terhadap perkiraan pengendalian (*controlling accounts*).
- Jawaban konfirmasi audit yang menunjukkan masalah.

4. Diversikasi kas (*Diversion of Cash*)

   Tanda peringatannya adalah:

   - Berkurangnya laba.
   - Gagal merekonsiliasi perkiraan bank.
   - Banyak memo kredit untuk menyesuaikan penjualan.
   - Penyesuaian yang signifikan terhadap perkiraan kas.

Pemahaman dan analisis lebih lanjut terhadap sinyal kecurangan *(red flag)* tersebut dapat membantu langkah selanjutnya untuk memperoleh bukti awal atau mendeteksi adanya tindakan kecurangan. Berikut adalah gambaran secara garis besar pendeteksian tindakan kecurangan berdasar penggolongan kecurangan oleh *Association of Certified Fraud Examinations* (*ACFE)*:

1. Tindakan Kecurangan atas Laporan Keuangan*.*

   Kecurangan dalam penyajian laporan keuangan umumnya dapat dideteksi melalui analisis laporan keuangan sebagai berikut:

   a. Analisis vertikal, yaitu teknik yang digunakan untuk menganalisis hubungan antara item-item dalam laporan laba rugi, neraca atau laporan arus kas dengan menggambarkannya dalam

persentase. Sebagai contoh, adanya kenaikan persentase hutang niaga dengan total hutang dari rata-rata 28% menjadi 52% di lain pihak adanya penurunan persentase biaya penjualan dengan total penjualan dari 20% menjadi 17% mungkin dapat menjadi satu dasar adanya pemeriksaan kecurangan.

b. Analisis horisontal, yaitu teknik untuk menganalisis persentasepersentase perubahan item laporan keuangan selama beberapa periode laporan. Sebagai contoh adanya kenaikan penjualan sebesar 80% sedangkan harga pokok mengalami kenaikan 140%. Dengan asumsi tidak ada perubahan lainnya dalam unsur-unsur penjualan dan pembelian, maka hal ini dapat menimbulkan sangkaan adanya pembelian fiktif, penggelapan atau transaksi ilegal lainnya.

c. Analisis rasio, yaitu alat untuk mengukur hubungan antara nilai-nilai item dalam laporan keuangan. Sebagai contoh adalah *current ratio,* adanya penggelapan uang atau pencurian kas dapat menyebabkan turunnya perhitungan rasio tersebut.

2. *Asset misappropriation* (Penyalahgunaan aset).

Teknik untuk mendeteksi tindakan kecurangan dalam kategori ini sangat banyak variasinya. Namun, pemahaman yang tepat atas pengendalian internal yang baik dalam pos-pos tersebut akan sangat membantu dalam melaksanakan pendeteksian tindakan kecurangan. Dengan demikian, terdapat banyak sekali teknik yang dapat dipergunakan untuk mendeteksi setiap kasus penyalahgunaan aset. Masing-masing jenis tindakan kecurangan dapat dideteksi melalui beberapa teknik yang berbeda.

Misalnya, untuk mendeteksi tindakan kecurangan dalam pembelian ada beberapa metode pendeteksian yang dapat digunakan. Metode tersebut akan sangat efektif apabila digunakan secara bersamaan. Setiap metode pendeteksian akan menunjukkan anomalis/gejala penyimpangan yang dapat diinvestigasi lebih lanjut untuk menentukan ada tidaknya kecurangan. Selain itu, metode tersebut akan menunjukkan kelemahan-kelemahan dalam pengendalian internal dan memberi peringatan pada auditor akan adanya potensi terjadinya tindakan kecurangan di masa mendatang. Metode yang digunakan adalah:

a. *Analytical review*

   Suatu *review* atas berbagai akun yang mungkin menunjukkan ketidakbiasaan atau kegiatan-kegiatan yang tidak diharapkan. Sebagai contoh adalah perbandingan antara pembelian barang persediaan dengan penjualan bersihnya yang dapat mengindikasikan adanya pembelian yang terlalu tinggi atau terlalu rendah apabila dibandingkan dengan tingkat penjualannya. Metode analisis lainnya adalah perbandingan pembelian persediaan bahan baku tahun sebelumnya dengan tahun sekarang yang mungkin mengindikasikan adanya kecurangan *overbilling scheme* atau kecurangan pembelian ganda.

b. *Statistical sampling*

   Sebagaimana persediaan, dokumen dasar pembelian dapat diuji secara *sampling* untuk menentukan ketidakbiasaan

(irregularities), metode pendeteksian ini akan efektif jika ada kecurigaan terhadap satu atributnya, misalnya pemasok fiktif. Suatu daftar alamat PO BOX akan mengungkapkan adanya pemasok fiktif

c. *Vendor or outsider complains*

Keluhan dari konsumen, pemasok atau pihak lain merupakan alat deteksi yang baik yang dapat mengarahkan auditor untuk melakukan pemeriksaan lebih lanjut.

d. *Site visit – observation*

Observasi ke lokasi biasanya dapat mengungkapkan ada tidaknya pengendalian internal di lokasi-lokasi tersebut. Observasi terhadap bagaimana transaksi akuntansi dilaksanakan kadangkala akan memberi peringatan pada auditor akan adanya daerah-daerah yang mempunyai potensi bermasalah.

2.2.3. Faktor yang Menyebabkan Tindakan Kecurangan

Terdapat banyak upaya internal yang menyebabkan kecurangan akan lebih sering atau cenderung terjadi di lingkungan kerja, seperti halnya sistem pengendalian internal yang lemah dalam perusahaan, kebijakan operasional yang kurang kuat dan kejujuran yang buruk di tingkat puncak dalam sebuah perusahaan (Bologna, 1993). Terdapat delapan faktor yang diidentifikasi oleh Bologna sebagai sebagai probabilitas atau kemungkinan penyebab terjadinya tindakan kecurangan yang makin meningkat, seperti: penghargaan yang kurang kuat, pengendalian manajemen yang kurang memadai dan kurangnya penegakkan aturan atau tata laksana umpan balik kinerja, kurang memadainya dukungan, kurang memadainya tinjauan operasional

perusahaan, kecerobohan terhadap aturan-aturan disipliner dalam perusahaan, situasi yang penuh perlawanan dan tetap dipertahankan, serta permasalahan motivasional lainnya. Jika pihak manajemen hanya memberikan sedikit perhatian kepada pegawai perusahaan dan sistem pengendalian internal mereka, maka tindakan kecurangan akan dilakukan oleh pihak internal dalam perusahaan yang memiliki akses terhadap aset dan sistem akuntansi perusahaan. Jumlah kerugian yang terjadi akan lebih tinggi apabila digunakan komputer untuk membantu pegawai perusahaan melakukan tindakan kecurangan. Sehingga, pengendalian komputer dan sistem pengendalian internal lainnya sangatlah penting untuk melindungi aset bisnis dalam perusahaan.

2.2.4. Tindakan Kecurangan pada Sistem Informasi Berbantuan Komputer (Perbankan)

Kemajuan teknologi serta peningkatan aktivitas kejahatan terorganisir, menyebabkan perusahaan dengan sistem informasi berbantuan komputer seperti perbankan mengalami kesulitan untuk mempertahankan keunggulan atas perilaku tindakan kecurangan. Praktik pencucian uang, kecurangan pinjaman (keterangan dokumen yang keliru, kecurangan pinjaman hipotek dan kecurangan pinjaman internal), kecurangan deposito dan cabang (penulisan cek kosong, manipulasi cek, pemalsuan cek, rekening baru, tempat penyimpanan uang, cek resmi/ pos wesel/wesel wisata, *hold-mail* serta rekening tidur), kecurangan transfer dana elektronik (transfer uang antar bank secara elektronik, transfer telepon, kecurangan kartu pembayaran dan Anjungan Tunai Mandiri/ATM), risiko orang dalam lainnya (kecurangan

akunting, kondisi yang memudahkan kecurangan dan penggelapan uang), tindakan kecurangan di dunia maya, kecurangan privasi, pencurian data, serta pencurian identifikasi — merupakan contoh dari tindakan kecurangan yang seringkali terjadi di bank yang telah maju dalam penggunaan teknologi informasi.

Kegagalan bank biasanya disebabkan karena tindakan kecurangan yang dilakukan pegawainya. Kesempatan untuk melakukan kecurangan disebabkan manajemen bank tidak berhasil menciptakan sistem internal dan kontrol eksternal yang baik. Peraturan-peraturan yang ada Undang-Undang N0. 25/2003 tentang Tindak Pidana Pencucian Uang serta aturan lain yang terkait dengan bank, mengharuskan personil yang terkait waspada untuk mendeteksi dan mencegah tindakan kecurangan di bank. Sebagai contoh, dengan adanya Undang-Undang tentang Tindak Pidana Pencucian Uang, harus ada peningkatan penyidikan dengan melaksanakan prosedur-prosedur mengenali pelanggan/nasabah yang baik. (Rohadian, 2008)

Kecurangan bank dapat diklasifikasikan dalam 2 kelompok besar, yaitu (Tunggal, 1994):

1. Kecurangan bank tanpa memanipulasi catatan-catatan bank *(non-concealments).* misalnya pencurian uang tunai dan surat-surat berharga oleh ”defrauder”.
2. Kecurangan oleh ”*embezzelers*” atau ”*defaulter*” dengan cara memanipulasi catatan-catatan bank, misalnya pengambilan terhadap perkiraan tidak aktif (*dormant accounts*) tanpa diotorisasi terlebih dahulu.

Kebijakan pengendalian tindakan kecurangan *(fraud control policy)* bank meliputi (Tunggal, 1994):

1. *Personal policy*, yaitu kebijakan yang mencakup seleksi, latihan, promosi dan remunerasi pegawai yang ketat.
2. *Functional control*, yaitu organisasi yang dikelompokkan menjadi beberapa bagian menurut fungsinya.
3. *Director's examination an outside auditors*, yaitu dilakukan audit bank oleh staf internal perusahaan maupun auditor eksternal secara rutin.
4. *Bond coverage*, misalnya adanya jaminan kasir atas risiko bila terjadi selisih kurang pada kas oleh kasir.

2.2.5. Metode Pendeteksian dan Pencegahan Tindakan Kecurangan

Tindakan kecurangan dapat memberikan beban utama berupa masalah pembiayaan bagi kebanyakan perusahaan. Berbagai metode pendeteksian dan pencegahan tindakan kecurangan saat ini digunakan untuk mengurangi biaya tidak langsung ataupun biaya langsung yang berkaitan dengan semua bentuk tindakan kecurangan. Beragam teknik yang terbukti efektif untuk pendeteksian dan pencegahan tindakan adalah (Biestaker, *et al.*, 2006):

1. Kode etik perusahaan atau kebijakan etika.
2. Tinjauan terhadap pengendalian internal dan peningkatannya.
3. Mengecek referensi pegawai.
4. Tinjauan terhadap kontrak pekerjaan.
5. *Fraud auditing.*
6. Kebijakan untuk melaporkan tindakan kecurangan.
7. Tinjauan atas kerawanan perusahaan atas tindakan kecurangan.
8. *Hot line service* untuk melaporkan tindakan kecurangan.

9. Kebijakan yang berkaitan dengan adanya *whistle-blowing*.
10. Operasional audit.
11. Penerapan akuntansi forensik oleh perusahaan.
12. Pelatihan pencegahan dan pendeteksian tindakan kecurangan.
13. Pelatihan etika.
14. Observasi atau pengamatan terhadap peralatan.
15. Meningkatkan perhatian pada manajemen senior dalam perusahaan.
16. Kode pemberian sanksi terhadap pemasok/rekanan.
17. Meningkatkan peranan komite audit.
18. Observasi terhadap korespondensi secara elektronis.
19. Kebijakan rotasi pegawai.
20. Departemen sekuritas.
21. Program bimbingan pegawai.
22. Tinjauan terhadap dana tunai perusahaan.
23. Observasi persediaan.
24. Rekonsiliasi laporan keuangan.
25. Etika terhadap petugas/pegawai.

(Metode selanjutnya berkaitan dengan penggunaan *software*)

26. Teknologi penetapan sampel untuk observasi atau deteksi.
27. *Data mining.*
28. Analisis digital.
29. Teknologi untuk audit berkelanjutan.
30. Teknologi untuk menghitung rasio keuangan
31. Teknologi perlindungan terhadap virus.
32. Perlindungan *password* atau kata sandi.

33. Teknologi perlindungan dengan metode *firewall*.
34. Teknologi untuk menyaring perangkat *software*.

Beberapa contoh metode pendeteksian dan pencegahan tindakan kecurangan di atas, diuraikan berikutnya.

2.2.5.1 Tinjauan terhadap Pengendalian Internal dan Peningkatannya

Pengendalian internal seringkali diperkirakan sebagai salah satu bentuk pertahanan utama dalam menghadapi bentuk tindakan kecurangan. Pengendalian internal dibentuk untuk menjaga dan memelihara kejujuran seseorang agar ia tetap bersikap jujur dan dalam lingkungan bersaing saat ini tidak semua perusahaan dapat mengupayakan untuk membahas permasalahan yang berkaitan erat dengan tindakan kecurangan. (Albrecht, 1994)

Sistem pengendalian internal tidak hanya didesain untuk mencegah tindakan kecurangan, tetapi juga untuk mendeteksi tindakan kecurangan bila hal ini terjadi. Sebuah sistem pengendalian internal yang efektif adalah sistem yang meliputi pengendalian yang bersifat preventif atau pencegahan, detektif atau untuk mendeteksi, dan korektif atau untuk pembetulan. Pihak manajemen dalam perusahaan bertanggung jawab terutama pada sistem pengendalian internal agar sistem ini tetap dipatuhi dan tetap berada di tempatnya dalam perusahaan, sehingga pengendalian dalam realitasnya atau dalam kenyataannya adalah pengendalian manajemen, bukanlah pengendalian akuntansi. Tujuan dari sistem pengendalian internal bukan untuk mengekang pegawai tetapi lebih ditujukan untuk memberikan sebuah lingkungan kerja di mana para pegawai yang baik akan tertantang untuk

melakukan sesuatu yang tidak umum atau sesuatu yang luar biasa. Agar pengendalian manajemen berhasil guna maka perlu diciptakan (Thompson,1992):

1. Sebuah lingkungan yang tidak akan mentolerir tindakan kecurangan terjadi dalam perusahaan.
2. Sebuah lingkungan yang melarang tindakan kecurangan untuk mengambil manfaat atau keuntungan dari perusahaan.
3. Pihak eksekutif, manajer dan para personil operasional terlatih lainnya untuk mengetahui adanya tindakan kecurangan dan gejala dari tindakan kecurangan tersebut.

2.2.5.2 Mempertahankan Kebijakan untuk Melaporkan Tindakan Kecurangan

Setiap perusahaan sebaiknya menciptakan dan mempertahankan kebijakan dalam melaporkan adanya tindakan kecurangan untuk memandu para pegawainya. Sebuah kebijakan atas tindakan kecurangan yang diterapkan oleh perusahaan sebaiknya dibuat secara terpisah dan berbeda dari kode etik perusahaan atau kebijakan etika. Model atau sampel dari kebijakan akan adanya tindakan kecurangan disediakan oleh *ACFE.* Kebijakan atas adanya tindakan kecurangan semacam ini dapat dikomunikasikan secara jelas pada pegawai. Beragam cara komunikasi meliputi penerapan orientasi untuk memperkerjakan pegawai baru, seminar pelatihan pegawai dan evaluasi kinerja tahunan. Pengakuan secara tertulis dari masing-masing pegawai dalam perusahaan menyatakan bahwa kebijakan yang telah dibaca dan dipahami sangatlah diperlukan.

2.2.5.3 *Hot Line Service* untuk Melaporkan Tindakan Kecurangan

Pendekatan terhadap pendeteksian tindakan kecurangan yang saat ini makin umum digunakan adalah dengan membuat *hot line service* yang bersifat rahasia (Holtfreter, 2004). Teknik ini juga sangat efektif dalam permasalahan biaya untuk pendeteksian adanya tindakan kecurangan atas hal yang berhubungan dengan pekerjaan dan tindakan menyimpang lainnya. Sebuah *hot line service* memungkinkan pegawai untuk memberikan informasi internal yang bersifat rahasia, tanpa perlu merasa takut akan adanya sanksi ataupun hal yang sifatnya membalas dendam dari pihak yang diduga melakukan tindakan kecurangan (Pergola *and* Sprung, 2005).

Layanan *hot line service* bisa dilakukan dalam perusahaan tersebut atau disediakan oleh pihak ketiga dalam perusahaan. Sebuah contoh dari layanan *hot line service* dari pihak ketiga adalah adanya pelayanan berlangganan dari *ACFE.* Hasil dari layanan telepon ini akan diberikan pada pihak klien dalam jangka waktu dua hingga tiga hari. Layanan *hot line service* ini tidak hanya menjadi alat pendeteksi yang efektif tetapi juga dapat meningkatkan pencegahan atas tindakan kecurangan. Pembentukan *hot line service* berpotensi memberikan pendapat atau opini kedua guna mempertimbangkan risiko kemungkinan akan diperkarakan.

2.2.5.4 Mengecek Referensi Pegawai

Perusahaan dalam melakukan pengujian atau pengecekan terhadap referensi pegawai biasa dilakukan sebelum mempekerjakan seorang pegawai dalam perusahaan. Pegawai dengan sejarah pernah terlibat atau melakukan tindakan kecurangan mungkin akan pindah dari satu perusahaan ke

perusahaan lainnya. Apabila referensi pegawai tidak dicek atau diuji kembali, maka besar kemungkinannya perusahaan mempekerjakan orang yang tidak jujur. Pegawai yang tidak jujur dapat mengambil keuntungan dari perusahaan yang tidak mencurigainya dengan mengambil keuntungan bernilai besar dan berpindah ke perusahaan baru atau pribadi sebelum tindakan kecurangan yang dilakukan terungkap. Resume dari para pegawai sebaiknya ditelaah dan diteliti dengan mendalam dan informasi yang diberikan oleh pegawai tersebut diverifikasi untuk menentukan apakah informasi yang diberikan oleh pegawai tersebut sah atau tidak. Perusahaan sebaiknya tidak hanya bergantung pada nomor telepon yang dapat dihubungi yang dicantumkan pada resume pekerjaan dari perusahaan sebelumnya, karena mungkin saja nomor telepon tersebut adalah fiktif. Nomor telepon perusahaan sebelumnya, sebaiknya didapatkan oleh perusahaan secara independen jangan hanya bergantung dari informasi pegawai semata.

Perusahaan sebaiknya melakukan cek referensi kedua, enam bulan setelah pegawai tersebut mulai bekerja. Alasan pemecatan terhadap pegawai yang tidak jujur dari pekerjaan sebelumnya mungkin belum memberikan waktu yang cukup untuk menjadi bagian dari laporan pegawai saat pengecekan awal dilakukan. Hal ini dapat dilakukan pada pengecekan yang kedua.

2.2.5.5 Tinjauan terhadap Kerawanan Perusahaan akan Tindakan Kecurangan.

Tinjauan terhadap kerawanan perusahaan atas suatu tindakan kecurangan sebaiknya diterapkan. Hal ini meliputi penilaian aset perusahaan

yang dipegang oleh perusahaan saat ini dan bagaimana aset tersebut digunakan dengan tidak tepat. Untuk perusahaan yang terlibat dalam pelayanan jasa via elektronis, maka tinjauan terhadap kerawanan perusahaan sebaiknya juga meliputi penilaian terhadap tindakan pegawai, kerugian yang terjadi akibat lembar kerja neraca yang tidak sesuai dengan data konsumen dan informasi keuangan lainnya. Tujuan dari peninjauan semacam ini adalah untuk mengatasi adanya pelaku tindakan kecurangan. Tinjauan terhadap kerawanan perusahaan dapat membantu untuk mengarahkan rencana auditor internal dan secara khusus menekankan pada aset yang sifatnya paling rawan. Tinjauan ini dianggap sebagai langkah proaktif dalam mencegah dan mendeteksi tindakan kecurangan. Pertimbangan dan penilaian terhadap kerawanan aset perusahaan tersebut akan membantu seorang auditor atau akuntan untuk melihat apa yang diinginkan oleh seorang penipu atau pencuri. Langkah yang diambil sebaiknya dapat mengeliminir, meminimalkan atau setidaknya mengendalikan tindakan kecurangan.

2.2.5.6 Tinjauan terhadap Kontrak Pekerjaan

Tinjauan terhadap kontrak perusahaan terhadap perjanjian yang mereka buat dapat memberikan indikasi kemungkinan adanya tindakan kecurangan kontrak, termasuk tindakan penyuapan atau konflik kepentingan lainnya dari pihak pegawai perusahaan. Kecurangan kontrak dapat terjadi saat rekan kerja melakukan tindakan kecurangan dan dengan sengaja mengambil keuntungan dari kontrak yang mereka buat dengan perusahaan dengan tujuan untuk memperoleh laba yang tidak sah. Kecurangan kontrak

mungkin melibatkan konspirasi antara personil perusahaan dan rekan kerja atau konspirasi antara dua pihak atau lebih.

Dengan menganalisa dokumen kontrak secara rutin pada penawaran terakhir, penawaran terendah atau pada saat memperoleh kontrak, dapat mendeteksi adanya kecurangan kontrak. Kontrak yang bernilai tinggi harus ditelaah, sering kali lalai atas kontrak kepada pihak rekan yang secara teratur melakukan kontrak, dengan andanya kemudahan yang sifatnya instan misalnya. Tinjauan semacam ini mungkin dapat mengungkapkan adanya tindakan penyuapan yang menjadi alasan diberikannya kemudahan tersebut. Beragam tinjauan terhadap laporan publik mungkin dapat mengungkapkan apakah pegawai memiliki kepentingan tersembunyi atas kontrak tersebut.

2.2.5.7 Teknologi Perlindungan terhadap *Password*

Pertumbuhan internet dan pelayanan jasa via elektronis menyebabkan peningkatan pada sejumlah jaringan komputer yang akhirnya dapat meningkatkan terjadinya tindakan kecurangan. Akuntan dan pihak investigator sebaiknya memastikan bahwa mereka merupakan pemakai yang sah dan memiliki akses terhadap jaringan komputer dengan data terkait. Meskipun *password* atau kata sandi merupakan pertahanan terhadap data komputer yang paling tua, tetapi cara ini masih terbukti efektif dan efisien sebagai metode untuk mengendalikan akses terhadap data.

Kelemahan atau kesulitan dengan adanya *password* atau kata sandi ini adalah adanya hubungan berlawanan antara membuat *password* yang efektif dan bisa dipergunakannya *password* tersebut. Jika persyaratan *password* terlalu kompleks atau rumit, maka pihak pengguna akan kesulitan

dalam menuliskan *password*-nya, hal ini justru menimbulkan risiko (Gerard, *et al.*, 2004). *Password* sebaiknya terdiri dari enam hingga delapan karakter dengan kombinasi huruf yang diacak, atau kombinasi angka maupun simbol yang diacak. Pengguna *password* sebaiknya diminta untuk sering-sering mengubah *password*-nya, misalkan 30 hingga 60 hari sekali. Selain itu, pihak pengguna sebaiknya juga melakukan siklus terhadap 6 hingga 12 *password* yang berbeda sebelum menggunakannya kembali (Gerard, *et al.*, 2004). Pegawai juga sebaiknya tidak diijinkan untuk memperlihatkan *password*-nya di lokasi-lokasi tertentu di mana kemungkinan terdapat individu yang tidak berwenang dapat melihatnya. Prosedur pemblokiran sebaiknya diterapkan jika pengguna gagal memasukkan *password* yang tepat setelah mencoba sebanyak tiga kali.

Teknologi sudah meningkatkan penciptaan bentuk perlindungan *password* terbaru dengan menggunakan ciri biologis dari si pengguna *password* (biometrik) seperti *password* dengan menggunakan suara, sidik jari, bentuk retina mata dan tanda tangan digital. Bentuk perlindungan *password* terbaru ini cederung lebih efektif dalam hal pembiayaan untuk masa mendatang.

2.2.5.8 Teknologi Perlindungan dengan Metode *Firewall*

Satu teknik penting untuk mengendalikan adanya akses data oleh pihak yang tidak berwenang adalah penggunaan metode *firewall*. Metode *firewall* dapat digunakan pada tingkatan *hardware* dan *software*. Pada tingkatan *software*, terdapat beberapa program khusus (seperti ZoneAlarm dari zonelabs.com) yang dapat dikoordinasikan dengan program *software*

yang terkait dengan internet (seperti *browsing*, *e-mail* dan lain sebagainya) untuk melindungi data. Perangkat *hardware* atau perangkat *software* mencegah seseorang agar tidak menemukan adanya sambungan atau akses ke perusahaan lewat internet. Sambungan internet dikenal dengan nama *Internet Protocol (IP).* Perangkat *hardware* atau *software* umumnya menyembunyikan alamat *IP* sehingga *cracker* tidak bisa menemukan dan mengakses data tersebut (Gerard, *el al.*, 2004).

2.2.5.9 Analisis Digital

Analisis digital berdasarkan pada Hukum Benford untuk menguji transaksi kecurangan berdasarkan pada apakah digit yang muncul di tempat tertentu dalam bentuk angka sudah sesuai dengan proporsi yang ada. Penyimpangan yang signifikan dari ekspektasi biasanya akan terjadi di bawah dua kondisi. Kondisi pertama adalah bahwa orang tersebut menambahkan satu observasi yang belum disesuaikan sebelumnya. Kondisi kedua adalah bahwa seseorang menghapuskan observasi data yang tidak menyertakan distribusi Benford (Durstchi, *et al.*, 2000).

Tindakan kecurangan pada pajak, kecurangan cek dan tindakan penipuan lain jelas akan menghasilkan nomor acak yang tidak dapat diketahui. Akuntan forensik dan para auditor sebaiknya menggantungkan pada ciri khas atau kebiasaan seseorang dan beragam jenis perangkat *software* untuk melakukan analisis digital, termasuk *DATS*, yang sudah terbukti mampu mengarah pada kebiasaan atau ciri khas dari seseorang (Lanza, 2000).

Jenis tindakan kecurangan lainnya yang tidak dapat dideteksi dengan menggunakan analisis digital karena datanya masih dalam pengujian. Misalkan, masih adanya dua alamat yang sama, rekening bank yang tidak bisa masuk ke data serta tidak bisa mendeteksi tindakan kecurangan seperti halnya manipulasi kontrak dan pengiriman barang yang sifatnya merugikan.

2.3. Penelitian Terdahulu

Penelitian sebelumnya yang membahas tentang pendeteksian tindakan kecurangan dan metode pencegahannya sudah mengacu pada penerapan pendekatan *red flag* (*fraud indicator*/sinyal kecurangan). Misalkan, Albrecht *and* Romney (1986) yang menyatakan dalam sebuah survei tentang para praktisi auditor yang menyatakan ada sekitar 31 standard yang berhubungan dengan pengendalian internal dalam perusahaan dan dianggap sebagai alat untuk memprediksi adanya tindakan kecurangan yang lebih baik. Survei yang dilakukan ini berbentuk daftar dengan 87 *red flag* (sinyal kecurangan). Loebeckke *and* Willingham (1988) menawarkan sebuah model yang dapat mempertimbangkan probabilitas dari adanya kesalahan penulisan pada laporan keuangan dikarenakan adanya tindakan kecurangan yang mengandung tiga faktor berikut:

1. Tingkat di mana pihak berwenang dalam perusahaan memiliki alasan untuk terlibat dalam tindakan kecurangan di bidang manajemen.
2. Tingkat di mana terdapat kondisi yang memungkinkan terjadinya tindakan kecurangan di mana pihak manajemen perusahaan akan terlibat di dalamnya.

3. Keberadaan pihak berwenang yang memiliki sikap atau nilai etika yang akan memfasilitasi kemungkinan terjadinya tindakan kecurangan.

Loebbecke *and* Willingham (1989) menggunakan pendekatan *red flag* untuk mengembangkan model atau konsep asli untuk mengevaluasi probabilitas atau kemungkinan adanya tindakan kecurangan. Sebuah instrumen penelitian berupa survei yang digunakan untuk menanyakan pada 27 rekan audit dari enam perusahaan besar. Para peneliti menyimpulkan bahwa penilaian auditor terhadap pengendalian internal dalam perusahaan klien akan lebih signifikan untuk mengevaluasi probabilitas atau kemungkinan terjadinya tindakan kecurangan. Pincus (1989) menemukan bahwa auditor yang tidak menerapkan pendekatan daftar *red flag* akan memiliki kinerja yang lebih baik dalam sebuah bentuk studi eskperimental. Dalam studi lainnya, auditor dinyatakan memiliki opini atau pendapat yang berbeda berkaitan dengan tingkat risiko terjadinya tindakan kecurangan yang diindikasikan dari berbagai indikator *red flag*. Auditor dengan pengalaman terhadap perusahaan klien yang berbeda dinyatakan memiliki persepsi yang berbeda pula tentang pentingnya indikator dari pendekatan *red flag* (Haskenbrack, 1993).

Peneliti lainnya sudah menelaah efektivitas dari beragam prosedur audit dalam mendeteksi tindakan kecurangan. Hylas *and* Ashton (1982) melakukan sebuah studi empiris dengan 281 kesalahan yang memerlukan penyesuaian laporan keuangan terhadap sekitar 152 audit. Para peneliti ini menyatakan bahwa prosedur peninjauan secara analitis dan diskusi dengan perusahaan klien akan memberikan prediksi atau perkiraan persentase besarnya kesalahan yang terjadi. Wright *and* Ashton (1989) menelaah

efektivitas dari metode pendeteksian tindakan kecurangan dari jawaban perusahaan klien. Ekspektasi didapatkan berdasarkan pada penelitian tahun sebelumnya dan tinjauan analitis didapatkan dari sampel sebanyak 186 tindakan yang melibatkan sekitar 368 penilaian audit. Peneliti ini mengemukakan bahwa sekitar setengah dari kesalahan tersebut terjadi dan disinyalir dari adanya tiga prosedur tercatat.

Blocher (1992) menemukan bahwa hanya empat dari 24 kasus tindakan kecurangan yang disinyalir melalui prosedur analitis. Calderon *and* Green (1994) menemukan bahwa prosedur analitis merupakan sinyal utama dengan tingkat persentase sebesar 15 persen dari 455 kasus adanya tindakan kecurangan. Kaminski dan Wetzel (2004) melakukan sebuh uji longitudinal dengan menggunakan beragam rasio keuangan yang terdiri dari 30 perusahaan yang saling dipasangkan. Dengan menggunakan metodologi teori *chaos*, uji metriks dilakukan untuk menganalisa perilaku dari data *time-series*. Para peneliti ini tidak menemukan adanya perbedaan dalam dinamika antara perusahaan yang melakukan tindakan kecurangan dan perusahaan yang tidak melakukan tindakan kecurangan dengan memberikan bukti adanya kemampuan rasio keuangan yang terbatas untuk mendeteksi adanya tindakan kecurangan.

Apostolou, *et al.* (2001) melakukan survei terhadap 140 auditor eksternal dan auditor internal terhadap faktor risiko adanya tindakan kecurangan dengan membuat dokumentasi tentang karakteristik manajemen sebagai alat prediksi yang paling signifikan atas tindakan kecurangan yang diikuti dengan operasionalisasi perusahaan klien ataupun fitur stabilitas keuangan dan kondisi industri. Chen *and* Senneti (2000) menerapkan sebuah

sistem audit yang strategis dengan karakteristik industri yang spesifik dan terbatas serta menggunakan model logistik regresi terhadap pasangan sampel dari 52 perusahaan yang diduga melakukan tindakan kecurangan terhadap laporan keuangan oleh pihak *Securrity and Exchange Comission (SEC).* Model yang diperoleh berdasarkan pada tingkat prediksi secara keseluruhan dengan tingkatan sebesar 91 persen untuk perusahaan yang melakukan tindakan kecurangan dan perusahaan yang tidak melakukan tindakan kecurangan.

Moyes *and* Baker (2003) melakukan sebuah survei yang terdiri dari para praktisi auditor yang mencemaskan tentang efektivitas dari metode pendeteksian tindakan kecurangan terhadap 218 standar prosedur audit. Hasil akhir yang diperoleh memberikan indikasi bahwa sekitar 56 dari 218 prosedur dianggap lebih efektif dalam mendeteksi adanya tindakan kecurangan. Secara umum, prosedur yang paling efektif adalah prosedur yang memberikan hasil sebuah bukti tentang adanya kekuatan dari pengendalian internal dalam perusahaan.

Binhadi (2005), dalam penelitiannya pada sistem informasi berbantuan komputer di Bank Mandiri, menyatakan bahwa kebijakan dasar dalam menyusun sistem pengendalian internal bank meliputi: (1) tujuan pengendalian internal bank; (2) manajemen risiko; (3) sistem dan prosedur. Berdasarkan kebijakan tersebut dan perlunya pengendalian berjenjang, aspek yang diperlukan meliputi:

1. *Supervisory board control* (pengawasan oleh dewan komisaris). Dewan komisaris bank bertanggung jawab mengawasi pelaksanaan pengendalian

internal secara umum dan memberikan nasehat kepada direksi melalui pengawasan preventif, represif dan penilaian berkala.

2. *Management control* (pengendalian vertikal). Direksi bertanggung jawab menciptakan dan memelihara sistem pengendalian internal yang efektif dan memastikan bahwa sistem tersebut berjalan dengan aman dan sehat.
3. *Built-in control*, tercermin dari adanya *segregation of duties*, *policy* manual, *standard operating procedure*, proses kerja melalui pola *prepares*, *checker and approval*, *transaction control*, serta mendorong terciptanya *risk culture*.
4. *Internal independent control system*, yang dilakukan oleh auditor internal secara *ex-post* dan *compliance/quality assurance* secara *ex-ante.*
5. Auditor independen, pemeriksaan yang dilakukan oleh Akuntan Publik sekurang-kurangnya setahun sekali.
6. Pengawasan dan pembinaan oleh otoritas pegawasan, mencakup aspek ketentuan perizinan dan kehati-hatian, *on-site* and *off-site* supervision serta *risk based supervision* untuk menjaga kepercayaan masyarakat terhadap perbankan.

Biestaker, *et al.* (2006) melakukan survei terhadap 86 akuntan, auditor internal dan para penyelidik akuntan bersertifikasi yang bertugas menelaah tindakan kecurangan. Penelitian ini menunjukkan ke-34 metode pendeteksian dan pencegahan tindakan kecurangan yang diteliti terbukti efektif menurut persepsi responden.

Perbedaan penelitian ini dengan penelitian sebelumnya terletak pada model penelitian dan objek yang menjadi sampel penelitian. Model penelitian

ini untuk membuktikan secara empiris bahwa persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Objek pertama ditujukan kepada kaum akademisi. Hal ini ditujukan untuk pengembangan ilmu pengetahuan pada pendidikan akuntansi. Objek kedua difokuskan pada pelaku sistem informasi berbantuan komputer, karena responden memiliki pengetahuan yang lebih memadai mengenai metode pendeteksian dan pencegahan tindakan kecurangan dengan penggunaan komputer.

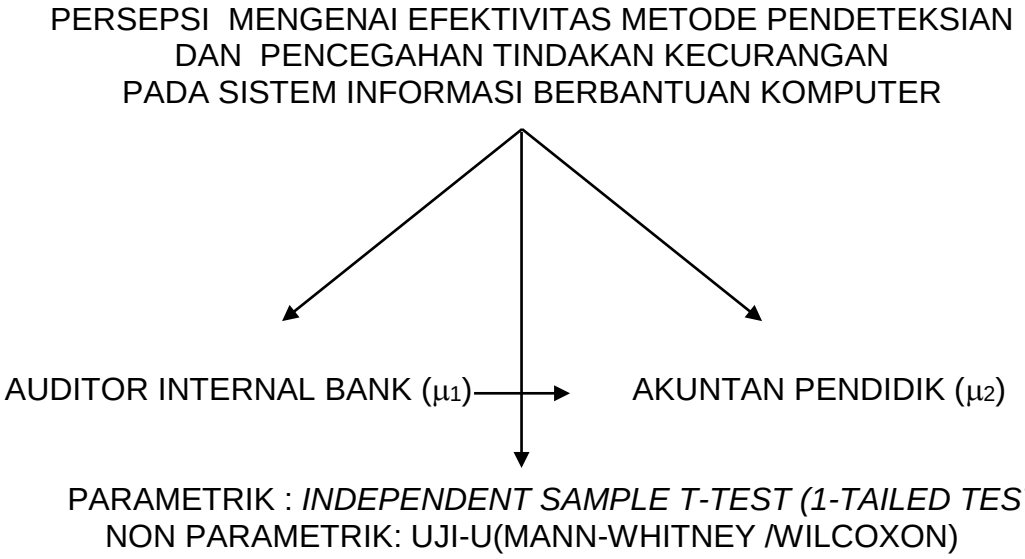
2.4. Kerangka Pemikiran Teoritis dan Hipotesis Penelitian

Persepsi auditor internal bank mengenai efektivitas metode pendeteksian tindakan kecurangan dan pencegahannya kemungkinan lebih baik dari akuntan pendidik. Faktor yang mendasarinya adalah pendidikan dan pengalaman operasional yang spesifik dari auditor internal bank. Hal ini disebabkan karena perbankan sangat intensif dalam melakukan perbaikan terhadap kinerja auditor internalnya, seperti adanya pemuktahiran Standar Pelaksanaan Fungsi Audit Intern Bank (SPFAIB) oleh Bank Indonesia dengan Peraturan Bank Indonesia No. 1/6/PBI/99 tanggal 20 September 1999. Untuk dapat mewujudkan profesionalismenya, khusus auditor internal bank, baik secara sendiri-sendiri ataupun bersama-sama, salah satunya harus mempunyai pengetahuan yang memadai dalam bidang tugasnya yaitu pengetahuan mengenai teknis audit dan disiplin ilmu lain yang relevan dengan spesialisasinya. Persyaratan minimal pendidikan bagi auditor internal bank ditetapkan oleh masing-masing bank sesuai dengan ukuran organisasi

maupun tingkat kerumitan kegiatan banknya. Meskipun demikian agar dapat melaksanakan tugasnya dengan baik, latar belakang pendidikan auditor internal bank seharusnya dapat menunjang untuk: (a) memahami penerapan SPFAIB; (b) memahami standar akuntansi keuangan; (c) memahami peraturan perundang-undangan yang berkaitan dengan kegiatan operasional perbankan; (d) memahami prinsip-prinsip manajemen khususnya manajemen perbankan, (e) memiliki pengetahuan mengenai ilmu yang berkaitan dengan kegiatan perbankan seperti ilmu ekonomi, ilmu hukum, perpajakan dan masalah-masalah keuangan, metode kuantitatif/statistik dan memahami prinsip-prinsip pengolahan data elektronik. Begitu juga pengalaman kerja yang memadai dalam bidang operasional perbankan akan menambah atau membantu memberikan kemahiran profesional bagi auditor internal bank.

Penelitian ini modifikasi dari penelitian yang sudah ada. Penelitian yang dilakukan Biestaker, Richard *and* Carl (2006) secara deskriptif menjelaskan berapa prosentase penggunaan metode pedeteksian dan pencegahan tindakan kecurangan yang dianggap efektif, serta efektivitas dari metode tersebut. Didasari oleh penelitian yang dilakukan Biestaker, *et al.* (2006) dan logika pemikiran teoritis yang ada dikembangkan model penelitian sebagai berikut:

Gambar 2.2.
Kerangka Pemikiran Teoritis



Dari model penelitian tersebut, dirumuskan hipotesis sebagai berikut:

H_A : Persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

BAB III
TUJUAN DAN MANFAAT PENELITIAN

3.1. Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Untuk mengetahui perangkat lunak yang digunakan pada metode dengan penggunaan komputer yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan.
2. Untuk mengetahui adanya metode baru berkaitan dengan penggunaan komputer yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan.
3. Menguji secara empiris persepsi yang lebih baik/tepat dari auditor internal bank, untuk mengukur ekfektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

3.2. Manfaat Penelitian

Penelitian ini diharapkan dapat berguna bagi pihak-pihak yang berkepentingan yaitu:

1. Dengan adanya identifikasi metode yang dapat bekerja dengan baik untuk pendeteksian dan pencegahan tindakan kecurangan, akan menghasilkan informasi yang bersifat preskriptif atau menjelaskan. Informasi ini berguna bagi auditor yang bertugas untuk melakukan pemeriksaan.
2. Bagi Ikatan Akuntan Indonesia, sebagai bahan masukan dan pertimbangan untuk mengambil langkah, tindakan maupun kebijakan

berkaitan dengan metode pendeteksian dan pencegahan tindakan kecurangan.

3. Bagi Bank Indonesia, dapat digunakan sebagai bahan untuk pengambilan kebijakan berkaitan dengan metode pendeteksian dan pencegahan tindakan kecurangan.
4. Menjadi masukan bagi perguruan tinggi terutama fakultas ekonomi jurusan akuntansi untuk referensi mata kuliah auditing.

BAB IV
METODE PENELITIAN

4.1. Desain Penelitian

Penelitian ini merupakan penelitian yang mengacu pada penelitian sebelumnya. Instrumen pada penelitian Biestaker, *et al.(*2006) digunakan untuk mendeskripsikan penggunaan dan efektivitas metode pendeteksian dan pencegahan tindakan kecurangan. Kemudian dimodifikasi untuk menguji apakah terdapat perbedaan persepsi auditor internal bank dengan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Dikarenakan skala yang digunakan adalah skala interval, maka dapat dilakukan pengujian satu arah yang membuktikan apakah persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Berdasarkan hasil persepsi yang lebih baik, dapat ditunjukkan persepsi siapa yang paling tepat untuk mengukur ekfektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

Jenis data yang digunakan dalam penelitian ini adalah data primer, yakni data yang diperoleh dari sumber aslinya. Diperoleh melalui survei dengan cara mengirim kuesioner via kurir dan via pos kepada auditor internal yang bekerja di bank dan akuntan pendidik yang bekerja pada perguruan tinggi.

4.2. Populasi dan Teknik Pengambilan Sampel

Populasi adalah sekumpulan orang, kejadian, atau segala sesuatu yang menjadi sasaran penelitian (Sekaran, 2000), sedangkan sampel adalah bagian dari populasi yang akan mewakili untuk diteliti. Populasi dalam penelitian ini adalah auditor internal yang bekerja pada bank dan akuntan pendidik yang bekerja pada perguruan tinggi. Data responden yang berkaitan dengan akuntan pendidik diperoleh dari direktori perguruan tinggi yang menyelenggarakan Program Studi Akuntansi. Untuk auditor internal bank, respondennya bekerja pada unit Satuan Kerja Audit Intern (SKAI). Hal ini dikarenakan auditor internal tersebut telah melalui proses rekrutmen dan pelatihan, sesuai dengan Standar Kompetensi Kerja Nasional Internal Audit Bank (Ratmanto, dkk, 2008).

Populasi auditor internal bank dan akuntan pendidik tidak dapat diketahui pasti jumlahnya. Untuk kepentingan analisis dengan statistik, penulis menentukan jumlah minimum sampel sebanyak 30 responden untuk tiap jenis auditor. Hal ini memenuhi batas jumlah sampel, sesuai dengan teori *Central Limit Theorems* yang menyatakan bahwa jumlah sampel untuk mencapai kurva normal setidaknya adalah mencapai nilai 30 responden (Mendenhall *and* Beaver, 1992) dalam (Santosa, 2005).

Berdasarkan teori tersebut, dengan sampel sebanyak 30 serta *response rate* untuk akuntan sebesar 17% (Murtanto, 1999), maka kuesioner dikirimkan dengan jumlah minimal 176 (30 x 100/17 = 176,47) eksemplar untuk auditor internal bank atau akuntan pendidik.

Teknik penentuan sampel dalam penelitian ini adalah *purposive sampling*. *Purposive sampling* adalah teknik penentuan sampel dengan

pertimbangan tertentu (Sugiyono, 2005), yang diharapkan dapat mewakili populasinya dan tidak menimbulkan bias bagi tujuan penelitian. Sampel ditentukan dengan kriteria sebagai berikut :

1. Auditor internal bank yang bekerja pada unit Satuan Kerja Audit Intern (SKAI) di sepuluh bank umum berdasar total aset terbesar (*Indonesian Bank Statistics*, 2008). Kriteria dipilih pertimbangan sepuluh bank umum berdasar total aset karena memiliki kantor operasional yang banyak tersebar di seluruh wilayah Indonesia (Direktori Bank Indonesia, 2008) dan telah majunya penggunaan teknologi informasi (Binhadi, 2005).

   Tabel berikut menjelaskan peringkat sepuluh bank umum berdasarkan aset terbesar dan jumlah kantor cabangnya di Indonesia serta di Jakarta.

Tabel 4.1.
Peringkat Bank Umum Berdasarkan Aset,
April 2008

Miliar Rp

No.	Nama Bank	Total Aset	Pangsa terhadap Total Aset Bank Umum (%)
1.	PT Bank Mandiri TBK	281.911	14,46
2.	PT Bank Central Asia TBK	217.193	11,14
3.	PT Bank Rakyat Indonesia TBK	199.717	10,25
4.	PT Bank Negara Indonesia TBK	163.981	8,41
5.	PT Bank Danamon Indonesia TBK	91.189	4,68
6.	PT Bank Niaga	54.731	2,81
7.	PT Pan Indonesia Bank TBK	51.408	2,64
8.	PT Bank Internasional Indonesia TBK	50.430	2,59
9.	Citibank N.A	42.354	2,17
10.	PT Bank Permata TBK	41.559	2,13
TOTAL		1.194.474	61,27

Sumber: *Indonesian Bank Statistics,* Vol. 6, No. 5, April 2008

Tabel 4.2.
Jumlah Kantor Cabang Sepuluh Bank Umum
dengan Peringkat Aset Terbesar

No.	Nama Bank	Jumlah Kantor Cabang di Indonesia	Jumlah Kantor Cabang di Jakarta
1.	PT Bank Mandiri TBK	543	300
2.	PT Bank Central Asia TBK	806	282
3.	PT Bank Rakyat Indonesia TBK	1588	145
4.	PT Bank Negara Indonesia TBK	96	357
5.	PT Bank Danamon Indonesia TBK	272	99
6.	PT Bank Niaga	70	32
7.	PT Pan Indonesia Bank TBK	60	24
8.	PT Bank Internasional Indonesia TBK	153	87
9.	Citibank N.A	16	11
10.	PT Bank Permata TBK	141	83
TOTAL		3745	1420

Sumber: Direktori Bank Indonesia, 2008

Sampel untuk auditor internal bank dalam penelitian ini adalah yang bekerja pada unit SKAI di kantor pusat. Responden yang digunakan adalah auditor internal pada unit SKAI kantor pusat di Jakarta. Kriteria ini dipilih karena sepuluh bank umum dengan total aset terbesar, semua kantor pusatnya berada di Jakarta. Jumlah kuesioner yang diberikan, disesuaikan proporsinya dengan jumlah kantor cabangnya di Jakarta, dengan rumus:

$$\text{Untuk Bank X} = \frac{\text{Jumlah KC X di Jakarta}}{\text{Total KC di Jakarta}} \times \text{Kuesioner untuk AIB}$$

KC : Kantor Cabang
AIB : Auditor Internal Bank

$$\text{Misal, untuk Bank Mandiri} = \frac{300}{1420} \times 176$$

$$= 37{,}18 \text{ (37 kuesioner)}$$

2. Akuntan pendidik yang bekerja pada perguruan tinggi. Kriteria ini dipilih karena manfaat yang akan diperoleh untuk pengembangan ilmu

pengetahuan pada tingkat perguruan tinggi khususnya dan pada pendidikan akuntansi pada umumnya. Sampel untuk akuntan pendidik adalah responden pada perguruan tinggi di Semarang. Kriteria ini dipilih karena jumlah akuntan pendidik pada perguruan tinggi di Semarang yang menyelenggarakan Program Studi Akuntansi memenuhi kriteria jumlah sampel untuk tiap kelompok responden (masing-masing 176). Kuesioner tiap perguruan tinggi disesuaikan jumlahnya dengan banyaknya dosen pengajar pada Program Studi Akuntansi masing-masing perguruan tinggi. Berikut tabel perguruan tinggi penyelenggara Program Studi Akuntansi di Semarang beserta jumlah responden yang dijadikan sampel penelitian.

Tabel 4.3.

Perguruan Tinggi Penyelenggara Progdi Akuntansi di Semarang

No.	PT. Penyelenggara Progdi Akuntansi	Jumlah Responden
1	Universitas Diponegoro	20
2	Universitas Negeri Semarang	15
3	Politeknik Negeri Semarang	15
4	Universitas Islam Sultan Agung	15
5	Universitas STIKUBANK	15
6	Universitas 17 Agustus 1945 Semarang	10
7	Universitas Katolik Soegijapranata	10
8	Universitas Semarang	10
9	Universitas Dian Nuswantoro	10
10	Universitas Pandanaran	5
11	Universitas Muhammadiyah Semarang	5
12	Universitas Wahid Hasyim	5
13	Universitas AKI	5
14	IKIP Veteran Jawa Tengah	5
15	Sekolah Tinggi Ilmu Ekonomi Anindyaguna	5
16	Sekolah Tinggi Ilmu Ekonomi Widya Manggala	5
17	Sekolah Tinggi Ilmu Ekonomi Dharma Putra Semarang	5
18	Sekolah Tinggi Ilmu Ekonomi Bank Bpd Jawa Tengah	4
19	Sekolah Tinggi Ilmu Ekonomi Semarang	3
20	Sekolah Tinggi Ilmu Ekonomi Totalwin	3
21	Sekolah Tinggi Ilmu Ekonomi Pelita Nusantara	3
22	Akademi Akuntansi Effendi Harahap	3
TOTAL		176

Sumber: Direktori Perguruan Tinggi (2009)

4.3. Variabel Penelitian dan Definisi Operasional Variabel

4.3.1. Variabel Penelitian

Variabel dalam penelitian ini diukur dengan instrumen-instrumen yang telah digunakan oleh peneliti terdahulu. Variabelnya adalah:

X_1 : Persepsi auditor internal bank mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

X_2 : Persepsi akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

Tiap variabel bebas terdiri dari 34 indikator (x1 sampai dengan x34), yang merupakan persepsi auditor internal bank atau akuntan pendidik mengenai efektivitas dari 34 metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

4.3.2. Definisi Operasional Variabel

Persepsi adalah proses pemberian arti terhadap lingkungan seseorang di mana stimulus menggerakan indra yang mencakup penafsiran obyek atau tanda dari sudut pengalaman tersebut. Robins (1996) secara implisit menyatakan bahwa persepsi satu individu terhadap suatu objek sangat mungkin memiliki perbedaan dengan persepsi individu yang lain terhadap obyek yang sama.

Metode pendeteksian dan pencegahan tindakan kecurangan dalam penelitian ini diperoleh dari penelitian yang dilakukan oleh Biestaker,

et al.(2006). Terdiri dari 34 metode yang terbukti efektif untuk pendeteksian dan pencegahan tindakan kecurangan. Ke-34 metode ini telah disebutkan dalam tinjauan pustaka.

Instrumen yang digunakan dalam peneltian ini adalah kuesioner yang telah dikembangkan dari penelitian sebelumnya yaitu pada penelitian Biestaker, et al. (2006). Diukur melalui persepsi auditor internal bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer.

Auditor internal bank dalam penelitian ini adalah auditor bekerja pada unit Satuan Kerja Audit Intern (SKAI). Hal ini dikarenakan auditor internal tersebut telah melalui proses rekrutmen dan pelatihan, sesuai dengan Standar Kompetensi Kerja Nasional Internal Audit Bank (Ratmanto, dkk, 2008). Selain itu tidak bekerja sebagai pengajar pada suatu perguruan tinggi baik universitas maupun sekolah tinggi. Bisa bersertifikasi maupun tidak bersertifikasi dan tidak ada jenjang pendidikan minimal.

Akuntan pendidik dalam penelitian ini adalah staf pengajar pada perguruan tinggi baik universitas atau sekolah tinggi yang menyelenggarakan Program Studi Akuntansi. Hal ini dikarenakan pada jenjang perguruan tinggi kurikulumnya telah memuat materi tentang sistem akuntansi dan sistem informasi dari suatu perusahaan, serta *auditing*. Pendidikan minimal adalah sarjana akuntansi. Bisa memiliki sertifikasi akuntan dan sertifikasi lainnya maupun tidak. Selain itu tidak bekerja sebagai internal auditor dalam unit SKAI.

Untuk mengukur persepsi mengenai efektivitas metode pendeteksian

dan pencegahan tindakan kecurangan, digunakan pernyataan-pernyataan yang terdapat pada lampiran 1. Instrumen yang digunakan dalam penelitian ini diadopsi dan dimodifikasi dari penelitian Biestaker, Richard, *and* Carl (2006). Masing-masing responden diminta untuk memilih salah satu pilihan jawaban dari sangat tidak efektif sampai sangat efektif, dengan skor 1 sampai 5.

1 = Sangat tidak efektif

2 = Tidak efektif

3 = Cukup efektif

4 = Efektif

5 = Sangat efektif.

4.4. Lokasi dan Waktu Penelitian

Pengambilan sampel dilakukan di wilayah Jakarta dan Semarang karena memenuhi kriteria jumlah sampel dengan memperhitungkan *response rate*-nya. Waktu penelitian adalah empat bulan.

4.5. Prosedur Pengumpulan Data

Penelitian ini menggunakan survei. Data yang digunakan dalam penelitian, diperoleh dengan pendistribusian kuesioner yang diberikan kepada responden melalui kurir dan kantor pos. Sebelumnya telah dilakukan *pre-test* untuk mengetahui apakah kuesioner mudah dipahami. Caranya kuesioner dibagikan kepada tiga staf pengajar Program Studi Akuntansi Universitas Muria Kudus yang dipilih secara random. Berdasarkan jawaban secara lisan dari ketiga orang tersebut yang menyatakan paham dan lengkapnya pengisian, kuesiner layak untuk disebarkan.

Selanjutnya, kuesioner dikirimkan kepada manajer SKAI dan Pimpinan Program Studi Akuntansi untuk diteruskan pada para staf pengajarnya. Responden diminta mengembalikan kuesioner yang telah diisi, selambatnya dua minggu setelah kuesioner diterima. Kuesioner yang kembali diseleksi terlebih dahulu untuk melihat lengkap tidaknya terisi, sebagaimana dikehendaki untuk kepentingan analisis.

Langkah yang diambil untuk mengatasi rendahnya *response rate* adalah menghubungi responden melalui telepon guna memastikan kuesioner yang dikirimkan sudah diterima dan dimohonkan untuk diisi serta segera dikirim kembali. Untuk menghindari timbulnya keraguan responden dalam pengisian kuesioner ini, dalam surat permohonan diterangkan bahwa respon akan dirahasiakan, hanya diuraikan dalam bentuk ringkasan statistik dan identitas responden serta perusahaannya tidak akan diidentifikasi secara detail. Peneliti juga menyampaikan terima kasih sebagai penghargaan atas partisipasi yang diberikan.

4.6. Teknik Analisis

Untuk mengetahui secara tepat teknik analisis yang digunakan, perlu diuraikan karakteristik data dalam penelitian ini. Data berupa skala preferensi, responden diminta melakukan nilai/*rate* (satu sampai dengan lima) terhadap efektivitas metode pencegahan dan pendeteksian tindakan kecurangan pada sistem informasi berbantuan komputer. Tiap kategori menggambarkan tingkat preferensi yang sama, namun tidak dapat dinyatakan bahwa metode yang mendapat nilai lima, nilainya lima kali dari nilai satu. Skala pengukuran seperti ini disebut dengan skala interval. Uji statistik yang

sesuai dengan skala ini adalah semua uji statistik, kecuali yang mendasarkan pada rasio seperti koefisien variasi. (Ghozali, 2002)

Pengujian hipotesis dimaksudkan untuk mengetahui ada tidaknya perbedaan rata-rata persepsi di antara dua kelompok responden, yaitu auditor internal bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Karena diantara masing-masing kelompok responden yang diuji tersebut saling independen, maka pengujian dilakukan dengan menggunakan alat analisis *Independent Sample t Test* / uji t (Santosa, 2005). Skala interval menunjukkan preferensi, yang berarti tiap kategori jawaban memiliki nilai/*rate,* sehingga rata-rata persepsi dari kedua kelompok responden dapat menunjukkan persepsi siapa yang lebih baik *(one-tailed test).* Uji t digunakan untuk uji parametrik dua sampel independen dengan populasi yang memiliki distribusi normal dan diasumsikan varian populasinya sama (dengan *Levene Test*). Bila populasinya tidak terdistribusi secara normal digunakan uji non parametrik dengan Mann-Whitney (Uji-U/Wilcoxon). Formula untuk uji t adalah :

$$t = \frac{\text{rata-rata sampel pertama – rata-rata sampel kedua}}{\text{standar error perbedaan rata-rata kedua sampel}}$$

$$t = \frac{(\overline{X_1}-\overline{X_2})-(\mu_1-\mu_2)0}{\sqrt{S_p^2\left(\frac{1}{n_1}+\frac{1}{n_2}\right)}}$$

$$S_p^2 = \frac{(n_1-1)S_1^2+(n_2-1)S_2^2}{n_1+n_2-2}$$

keterangan :

$\overline{X_1}$ = rata-rata persepsi internal auditor S_p^2 = estimasi variasiasi gabungan

$\overline{X_2}$ = rata-rata persepsi eksternal auditor S_1, S_2 = deviasi standar

n_1, n_2 = jumlah sampel

(μ_1-μ_2)= beda dua rata-rata hitung populasi

Sebelum melakukan uji hipotesis terlebih dahulu dijelaskan mengenai statistik deskriptif, dilakukan uji respon bias, uji validitas dan reliabilitas instrumen, serta uji normalitas data. Apabila instrumen tersebut *valid* dan *reliable* (handal) maka hasil penelitian dapat menggambarkan keadaan sebenarnya.

4.6.1. Statistik Deskriptif

Statistik ini diperlukan untuk menunjukkan ukuran penyebaran data.

4.6.2. Analisis Deskriptif mengenai Perangkat Lunak yang Digunakan dan Metode Baru dengan Penggunaan Komputer

Analisis ini menjelaskan secara deskriptif atas data yang diperoleh mengenai perangkat lunak yang digunakan pada metode berbantuan komputer serta metode baru berbantuan komputer yang diperoleh dalam penelitian ini.

4.6.3. Uji *Non-Response Bias*

Pengujian *non-response bias* dilakukan dengan tujuan untuk melihat apakah karakteristik jawaban yang diberikan oleh responden yang ikut berpartisipasi (mengembalikan kuesioner) dengan responden yang tidak mau berpartisipasi (*non-response*) berbeda. Pengumpulan data melalui *mail survey* memungkinkan hal tersebut terjadi yang pada akhirnya akan berpengaruh pada hasil analisis data. Masalah ini akan semakin serius apabila tingkat pengembalian (*response rate*) sangat rendah.

Untuk mengatasi masalah ini, uji *non-response bias* dilakukan dengan cara membandingkan karakteristik antara responden yang ikut berpartisipasi (mengembalikan kuesioner) dengan responden yang tidak mau berpartisipasi (*non-response*) berdasarkan penentuan batas tanggal pengembalian kuesioner. Dengan menentukan responden yang mengembalikan kuesioner pada sebelum batas tanggal pengembalian (*early response*) dengan responden yang mengembalikan kuesioner setelah batas tanggal pengembalian (*late response*). Dilakukan uji-t untuk mengetahui ada tidaknya perbedaan signifikan antara responden yang mengembalikan kuesioner sebelum batas tanggal pengembalian dengan responden yang mengembalikan kuesioner setelah batas tanggal pengembalian. Apabila pengujian menunjukkan hasil *p-value*>0,05 berarti tidak ada perbedaan yang signifikan.

4.6.4. Uji Validitas

Menurut Ghozali (2002) uji validitas digunakan untuk mengukur sah atau valid tidaknya suatu kuesioner. Suatu kuesioner dikatakan valid jika pertanyaan pada kuesioner mampu untuk mengungkapkan sesuatu yang akan diukur oleh kuesioner tersebut. Dilakukan dengan melakukan *Corrected Item-Total Correlation*.

4.6.5. Uji Reliabilitas

Menurut Ghozali (2002) suatu kuesioner dikatakan reliabel atau handal jika jawaban seseorang terhadap pertanyaan adalah konsisten dari waktu ke waktu. Pengujian ini dilakukan dengan menghitung *cronbach alpha* dari masing-masing instrumen dalam suatu variabel. Instrumen dapat

dikatakan handal (*reliabel*) bila memiliki koefisien *cronbach alpha* lebih dari 0,60 (Nunnally, 1969 dalam Ghozali, 2002).

4.6.6. Uji Normalitas

Pengujian normalitas adalah pengujian tentang kenormalan distribusi data (Santosa, 2005). Untuk pengujiannya dapat menggunakan uji Kolmogorov-Smirnov. Jika nilai probabilitas lebih dari 0,05 maka nilai residualnya terdistribusi secara normal.

4.6.7. Uji Hipotesis

Hipotesis pengujiannya menggunakan uji beda rata-rata dengan uji *Independent Sample t-Test*. Dengan pengujian satu arah dapat diuji: persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer. Tahap-tahap pengujiannya sebagai berikut (Santosa, 2005):

1. Merumuskan pengujian hipotesis

   H_A: $\mu_1 \neq \mu_2$

   Dimana:

   μ = rata-rata persepsi auditor internal bank / akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan.

2. Menentukan level signifikansi

   Level signifikansi yang digunakan adalah 95% atau α = 0,05 untuk pengujian satu arah.

3. Menentukan jenis uji yang digunakan.

Jenis pengujian yang dilakukan adalah uji t untuk rata-rata dua sampel.

4. Menentukan aturan pengambilan keputusan.

   Aturan keputusan yang pertama (menguji kesamaan varian dua populasi), jika probablitas atau p(sig.F) > 0,05 maka ada kesamaan varian populasi dan jika p(sig.F) < 0,05 maka tidak ada kesamaan varian populasi. Apabila ada kesamaan varian populasi langkah selanjutnya dapat diambil. Pada skala interval, tiap kategori menyatakan nilai/*rate*, sehingga dapat menunjukkan persepsi yang lebih baik. Oleh karena itu, pengujian satu sisi *(one-tailed test)* dapat dilakukan. Tingat kepercayaan untuk uji ini adalah 95% atau alpha 5% (0,05). Selanjutnya, untuk aturan keputusan yang kedua (menguji signifikansi perbedaan rata-rata) adalah H_A diterima jika nilai p(sig.t)<0,05 dan H_A ditolak jika p(sig.t) > 0.05. (Budi, 2005)

   Pengambilan keputusan untuk pengujian signifikansi perbedaan rata-rata kedua populasi dapat menggunakan titik kritis. Dengan mencari pada tabel t, menggunakan derajat kebebasan (df) sebesar ukuran sampel satu dan dua dikurangi dua (n_1+n_2-2) pada taraf kepercayaan 95% (alpha 0,05), akan ditemukan nilai t sebagai titik kritis pengambilan keputusan. Jika $t_{Hitung} > t_{Tabel}$ maka menerima H_A dan jika $t_{Hitung} < t_{Tabel}$, maka H_A ditolak.

5. Menghitung nilai statistik.

   Tahap berikutnya adalah menghitung nilai statistik dengan menggunakan Program SPSS.

6. Pengambilan keputusan dan interpretasi hasil.

   Menentukan keputusan yang akan diambil dan menginterpretasikan hasil dari analisis data.

BAB V

HASIL PENELITIAN DAN PEMBAHASAN

5.1. Pengumpulan Data dan Demografi Responden

5.1.1. Pengumpulan Data

Data mengenai persepsi auditor internal bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan diperoleh dari hasil pengisian kuesioner yang dikirim via kurir dan pos. Jumlah responden auditor internal bank dan akuntan pendidik, dengan mempertimbangkan *respon rate*-nya 352 (176 x 2). Dari jumlah tersebut, yang kembali sebanyak 98 kuesioner dari auditor internal bank dan 73 kuesioner dari akuntan pendidik. Dari 98 kuesioner auditor internal bank yang kembali, sebanyak 61 yang sah untuk seterusnya dianalisis. Sedangkan dari 73 kuesioner akuntan pendidik yang kembali, 64 sah dan dipilih 61 secara acak untuk selanjutnya dianalisis.

5.1.2. Demografi Responden

Demografi responden merupakan karakteristik yang dimiliki oleh reponden, dilihat dari jenis kelamin, tingkat pendidikan dan pengalaman bekerja sebagai auditor internal bank/akuntan pendidik. Dari hasil jawaban responden dapat dilihat penjelasan di bawah ini:

a. Pengelompokan Responden berdasarkan Jenis Kelamin

Tabel 5.1.
Jenis Kelamin Responden

Jenis Kelamin	Auditor Internal Bank	Akuntan Pendidik	Total	Persentase
Pria	42	41	80	68,03%
Wanita	19	20	42	31,97%

Sumber: Data primer yang diolah

Berdasarkan tabel di atas, jenis kelamin auditor internal bank dan akuntan pendidik dari 122 responden yang digunakan sebagai sampel penelitian, sebagian besar adalah pria (68,03%) dan untuk wanita 31,97%.

b. Tingkat Pendidikan Responden

Tabel 5.2.
Tingkat Pendidikan Responden

Keterangan	Auditor Internal	Auditor Eksternal	Total	Persentase
Diploma	-	-	-	0%
Sarjana	49	1	50	40,98%
Pascasarjana	12	60	72	59,02%

Sumber: Data primer yang diolah

Berdasarkan tabel di atas, sebagian besar responden yang menyelesaikan pendidikan formalnya sampai dengan pascasarjana 59,02%. Sedangkan untuk sarjana 40,98% dan tidak ada dari diploma.

c. Pengalaman Bekerja

Tabel 5.3.
Pengalaman Bekerja

Keterangan	Auditor Internal Bank	Akuntan Pendidik	Total	Persentase
2-5 tahun	21	2	23	18,85%
Lebih dr 5 tahun	40	59	99	81,15%

Sumber: Data primer yang diolah

Berdasarkan tabel di atas, yang memiliki pengalaman bekerja lebih dari lima tahun adalah 81,15% dari keseluruhan responden. Sedang sisanya 18,85% adalah reponden dengan pengalaman bekerja dua sampai dengan lima tahun.

5.2. Statistik Deskriptif

Tabel 5.4.
Ukuran Penyebaran

Variabel	*N*	*Mean*	*Stdev*	*Min.*	*Max.*
Persepsi auditor mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan	122	3,6839	0,3705	2,8529	4,4412

Sumber: Data primer yang diolah

Tabel 5.4 menunjukkan ukuran penyebaran data dalam penelitian ini. Dari tabel tersebut, *N* atau jumlah data yang valid dari rata-rata persepsi auditor mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan atas 34 indikator variabel adalah sebanyak 122.

Dari 122 responden yang dijadikan sampel, persepsi mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan yang terkecil *(minimum)* adalah 2,8529 dan terbesar *(maximum)* adalah 4,4412. Rata-rata persepsi mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan dari 122 responden adalah 3,6839 dengan standar deviasi sebesar 0,3705.

5.3. Analisis Deskriptif Berkaitan dengan Metode Pendeteksian dan Pencegahan Tindakan Kecurangan

5.3.1. Efektivitas Metode Pendeteksian dan Pencegahan Tindakan Kecurangan Berdasarkan Persepsi Auditor Internal Bank dan Akuntan Pendidik

Persepsi auditor internal bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan terlihat dalam tabel 5.5.

Tabel 5.5.
Efektivitas Metode Pendeteksian dan Pencegahan Tindakan Kecurangan
(Persepsi Auditor Internal Bank dan Akuntan Pendidik)

Metode Pendeteksian dan Pencegahan Tindakan Kecurangan	Efektivitas Metode	*Rangking*
1. Kode etik perusahaan atau kebijakan etika.	3,5164	19
2. Tinjauan terhadap pengendalian internal dan peningkatannya.	3,8033	15
3. Mengecek referensi pegawai.	3,4508	23
4. Tinjauan terhadap kontrak pekerjaan.	2,8689	33
5. *Fraud auditing.*	4,3689	1
6. Kebijakan untuk melaporkan tindakan kecurangan.	3,2951	25
7. Tinjauan atas kerawanan perusahaan atas tindakan kecurangan.	3,3689	24
8. *Hot line service* untuk melaporkan tindakan kecurangan.	3,2213	27
9. Kebijakan yang berkaitan dengan adanya *whistle-blowing*.	4,2951	2
10. Operasional audit.	3,8934	13
11. Penerapan akuntansi forensik oleh perusahaan.	4,2459	3
12. Pelatihan pencegahan dan pendeteksian tindakan kecurangan.	3,8443	14
13. Pelatihan etika.	3,5738	18
14. Observasi atau pengamatan terhadap peralatan.	3,4918	21
15. Meningkatkan perhatian pada manajemen senior dalam perusahaan.	3,6803	17
16. Kode pemberian sanksi terhadap pemasok/rekanan.	4,0984	9
17. Meningkatkan peranan komite audit	4,1066	8
18. Observasi terhadap korespondensi secara elektronis.	3,0574	31
19. Kebijakan rotasi pegawai.	3,1066	28
20. Departemen sekuritas.	3,0820	30
21. Program bimbingan pegawai.	3,0902	29
22. Tinjauan terhadap dana tunai perusahaan.	3,5082	20
23. Observasi persediaan.	3,2623	26
24. Rekonsiliasi laporan keuangan.	4,1803	6
25. Etika terhadap petugas/pegawai.	2,9098	32
26. Teknologi penetapan sampel untuk observasi atau deteksi.	3,7295	16
27. *Data mining.*	4,1885	5
28. Analisis digital.	3,9098	12

29. Teknologi untuk audit berkelanjutan.	4,1557	7
30. Teknologi untuk menghitung rasio keuangan	3,4836	22
31. Teknologi perlindungan terhadap virus.	4,2377	4
32. Perlindungan *password* atau kata sandi.	4,0410	10
33. Teknologi perlindungan dengan metode *firewall*.	4,2459	3
34. Teknologi untuk menyaring perangkat *software*.	3,9426	11

Sumber: Data primer yang diolah
Keterangan: Nomor 26-34 adalah metode dengan penggunaan *software*

5.3.2. Penggunaan *Software* Pendeteksian dan Pencegahan Tindakan Kecurangan

Penjelasan berkaitan dengan metode pendeteksian dan pencegahan tindakan kecurangan dengan teknologi komputer dan *software* yang digunakan dapat dilihat pada tabel 5.6 berikut ini:

Tabel. 5.6.
Metode dengan Penggunaan *Software*

Metode Pendeteksian dan Pencegahan Tindakan Kecurangan	*Software* yang Digunakan
1. Teknologi penetapan sampel untuk observasi atau deteksi.	*Sniffing Software, Igor*
2. *Data mining*.	*Integral Solution Ltd's Clementine, Data Mine Corp's Data Crusher, IBM's Intelegent Miner*
3. Analisis digital.	*NSA, DAS, Rekayasa Oracle/Igres/Unify*
4. Teknologi untuk audit berkelanjutan.	*Audit Commmand Language (ACC)*
5. Teknologi untuk menghitung rasio keuangan	Rekayasa Software Rasio Keuangan Bank dari Borland *Dhepi, Template Excel*
6. Teknologi perlindungan terhadap virus.	*Visual Basic, Online Scanner, Threatfire,* Macam-Macam Anti Virus
7. Perlindungan *password* atau kata sandi.	*Morello Key Ring Password Protection Software, Multiple Users Prompt Software, Pasword Prompt Software, Three Tries Software*
8. Teknologi perlindungan dengan metode *firewall*.	*Visual Basic, DNS-Spoofing, Cache DNS,* Macam-Macam Anti Virus
9. Teknologi untuk menyaring perangkat *software*.	*Enologic Software, Antispyware Software, Anti Virus-Malware Protection*

Sumber: Data primer yang diolah

Hasil perolehan data, berkaitan dengan *software* yang digunakan pada metode pendeteksian dan pencegahan tindakan kecurangan diuraikan pada

tabel 5.6. Di samping itu terdapat metode baru berkaitan dengan penggunaan *software* dari hasil perolehan data, yaitu teknologi untuk mendeteksi verifikasi tanda tangan dengan menggunakan *Signature Verification System* (SVS).

5.4 Uji Asumsi Klasik

5.4.1. Uji *Non-Response Bias*

Pengujian ini dilakukan dengan tujuan untuk melihat apakah karakteristik jawaban yang diberikan oleh responden yang ikut berpartisipasi (mengembalikan kuesioner) dengan responden yang tidak mau berpartisipasi (*non-response*) berbeda. Seluruh kuesioner yang digunakan dalam penelitian ini diperoleh dalam batas waktu pengembaliannya, sehingga uji *non-response bias* tidak perlu dilakukan.

5.4.2. Uji Validitas

Uji validitas digunakan untuk mengukur sah atau valid tidaknya suatu kuesioner. Suatu kuesioner dikatakan valid jika pertanyaan pada kuesioner mampu untuk mengungkapkan sesuatu yang akan diukur oleh kuesioner tersebut. Dilakukan dengan melakukan *Corrected Item-Total Correlation*.

Berdasarkan tabel 4.10, dengan mencari nilai r_{Tabel} untuk uji satu sisi pada taraf kepercayaan 95% atau signifikansi 5% dan df (N-2)= 122-2 = 120, ditemukan nilai r_{Tabel}=0,1496. Syarat validitas data adalah $r_{Hitung} > r_{Tabel}$. Seluruh indikator variabel memiliki nilai r_{Hitung} *(Cronbach's Alpha if Item Deleted)* > 0,1496. Kesimpulan yang dapat diambil adalah seluruh indikator variabel (x1 sampai dengan x34) dinyatakan valid.

Tabel 5.7.
Hasil Uji Validitas

Indikator Variabel	*Cronbach's Alpha if Item Deleted*
x1	0.8250
x2	0.8223
x3	0.8263
x4	0.8272
x5	0.8202
x6	0.8269
x7	0.8279
x8	0.8277
x9	0.8206
x10	0.8157
x11	0.8210
x12	0.8185
x13	0.8244
x14	0.8260
x15	0.8220
x16	0.8196
x17	0.8210
x18	0.8251
x19	0.8263
x20	0.8237
x21	0.8234
x22	0.8243
x23	0.8244
x24	0.8191
x25	0.8266
x26	0.8196
x27	0.8190
x28	0.8174
x29	0.8170
x30	0.8291
x31	0.8195
x32	0.8211
x33	0.8204
x34	0.8166

Sumber: Hasil analisis

5.4.3. Uji Reliabilitas

Pengujian ini dilakukan dengan menghitung *cronbach alpha* dari masing-masing instrumen dalam suatu variabel. Instrumen dapat dikatakan handal (reliabel) bila memiliki koefisien *cronbach alpha* lebih dari 0,60.

Tabel 5.8.
Hasil Uji Reliabilitas

Cronbach's Alpha	*Cronbach's Alpha Based on Standardized Items*	*N of Items*
0,827	0,823	34

Sumber: Hasil analisis

Berdasarkan tabel 5.8, terlihat bahwa nilai *Cronbach's Alpha* adalah 0,827 dengan jumlah pertanyaan 34 butir/*item*. Hasil *Cronbach's Alpha* sebesar 0,827 ini menunjukkan nilai yang jauh di atas 0,60. Dapat disimpulkan bahwa reliabilitas dari konstruk atau variabel persepsi tinggi.

5.4.4. Uji Normalitas

Pengujian ini bertujuan untuk menguji apakah kedua variabel dalam penelitian mempunyai distribusi normal ataukah tidak. Normalitas dapat dideteksi dengan uji normalitas Kolmogorov-Smirnov dalam tabel 5.9 berikut ini:

Tabel 5.9.
Hasil Uji Kolmogorov-Smirnov

Kolmogorov-Smirnov Test

		Persepsi
N		122
Normal Parameters[a,b]	Mean	3.6839
	Std. Deviation	.37050
Most Extreme Differences	Absolute	.106
	Positive	.091
	Negative	-.106
Kolmogorov-Smirnov Z		1.176
Asymp. Sig. (2-tailed)		.126

a. Test distribution is Normal.

b. Calculated from data.

Sumber: Hasil analisis

Dari tabel di atas, dapat diinterpretasikan bahwa N=122 berarti jumlah sampel

yang diteliti adalah 122 data. Pada kolom variabel persepsi terdapat nilai Kolmogorov-Smirnov = 1,176 dengan probabilitas 0,126. Persyaratan nilai residual data tersebut normal jika probabilitas atau p > 0,05. Oleh karena p = 0,126 atau p > 0,05, maka diketahui bahwa nilai residual variabel persepsi pada 122 sampel terdistribusi secara normal, atau memenuhi persyaratan uji normalitas.

5.5. Pengujian Hipotesis dengan *Independent t–Test*

Dalam penelitian ini uji hipotesis dilakukan dengan uji-t. Pengujian ini dilakukan untuk menguji H_A: $\mu_1 \neq \mu_2$, menganalisis apakah terdapat perbedaan variabel independen persepsi auditor internal bank dan akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan. *Group Statistics* dan signifikansi hasil uji berdasarkan uji-t tampak dalam tabel 5.10 dan 5.11 berikut ini:

Tabel 5.10.
Group Statistics

Jenis Auditor	Jumlah Sampel	Rata-Rata Perspesi	Standar Deviasi	*Standard Error*
Internal	61	3,9581	0,25229	0,03230
Eksternal	61	3,4098	0,24578	0,03147

Sumber: Hasil analisis

Tabel 5.11.
Hasil Uji *Independent Sample t-Test*

Keterangan	*Levene's Test*		*t-test for Equality of Means*		
	F	Sig.	t	df	Sig.
Equal variances assumed	0,453	0,502	12,156	120	0,000

Sumber: Hasil analisis

Interpretasi pada *Group Statistic*: untuk auditor internal bank (AIB),

rata-rata persepsi 3,9581, standar deviasi 0,25229 dan rata-rata *standard error* 0,03230. Untuk akuntan pendidik (AP), rata-rata persepsi 3,4098, standar deviasi 0,24578 dan rata-rata *standard error* 0,03147.

Interpretasi pada *Independent Sample t-Test* yang pertama (pengujian kesamaan varian dua populasi dengan *Levene's Test*), keputusan yang diambil adalah pada *Equal Variances Assumed* F_{Hitung}=0,453; p(sig.)=0,502 yang berarti p > 0,05. Hasil dari Levene's Test menunjukkan varian dari dua populasi (AIB dan AP) adalah sama.

Interpretasi pada *Independent Sample t-Test* yang kedua adalah menguji perbedaan rata-rata persepsi kedua jenis auditor (AIB dan AP) dengan uji-t. Cara pertama dengan melihat pada nilai t_{Hitung}=12,156; nilai probalitasnya adalah 0,000. Oleh karena p < 0,05; maka H_A diterima atau rata-rata persepsi dari kedua jenis auditor (AIB dan AP) berbeda. Cara kedua dengan membandingkan nilai t_{Hitung}=12,156 dengan t_{Tabel}=1,658 (df=120 untuk tingkat kepercayaan 95% / alpha 0,05 pada pengujian satu arah; dicari dalam daftar tabel *t* pada **lampiran**), maka H_A diterima ($t_{Hitung} > t_{Tabel}$) atau terdapat perbedaan persepsi antara auditor internal dan eksternal mengenai efektivitas motode pendeteksian dan pencegahan tindakan kecurangan. Selanjutnya, berdasarkan rata-rata persepsi pada *Group Statistics* (rata-rata persepsi AIB > AP) dan hasil *Independent Sample t-Test* pada pengujian satu arah *(one-tailed test)*, maka hipotesis **persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan**, diterima.

5.6. Pembahasan

5.6.1. Pengetahuan Auditor Internal Bank dan Akuntan Pendidik Berkaitan dengan Efektivitas Metode Pendeteksian dan Pencegahan Tindakan Kecurangan beserta Perangkat Lunak yang Digunakan.

Berdasarkan persepsi auditor internal dan ekternal: *fraud auditing* (rata-rata efektivitas=4,3689), kebijakan yang berkaitan dengan adanya *whistle blowing* (4,2951) dan penerapan akuntansi forensik di perusahaan (4,2459) merupakan tiga dari metode pendeteksian dan pencegahan tindakan kecurangan yang memiliki tingkat efektivitas tertinggi. Sedangkan etika terhadap petugas/pegawai dan tinjauan terhadap kontrak pekerjaan merupakan metode yang memiliki rata-rata efektivitas terendah. Metode dengan efektivitas tertinggi berkaitan dengan teknologi penggunaan *software* yaitu teknologi perlindungan dengan metode *firewall* (4,2459). Peringkat selanjutnya adalah perlidungan *password* atau kata sandi (4,2377) dan *data mining*.

Terdapat beberapa temuan dalam penelitian ini, berkaitan dengan *software* yang digunakan untuk pendeteksian dan pencegahan tindakan kecurangan seperti yang telah dijelaskan pada tabel 5.6. Termasuk ditemukannya metode baru yaitu teknologi untuk mendeteksi verifikasi tanda tangan dengan menggunakan *Signature Verification System* (SVS). Pengetahuan dan keterampilan yang memadai dari para pelaku sistem (Auditor Internal Bank) maupun kaum akademisi (Akuntan Pendidik) mengenai metode tersebut dan *software* yang digunakan sudah menjadi tuntutan era dimana *fraud* berkembang sangat maju.

Hasil penelitian ini berbeda dengan penelitian Biestaker, *et al.*(2006), yang melakukan survei terhadap 86 akuntan, auditor internal dan para penyelidik akuntan bersertifikasi yang bertugas menelaah tindakan kecurangan. Hasil penelitian Biestaker menjelaskan penerapan akuntansi forensik oleh perusahaan, teknologi perlindungan terhadap virus dan perlindungan dengan *firewall*, merupakan metode yang paling efektif untuk pendeteksian dan pencegahan tindakan kecurangan. Lokasi dan waktu penelitian yang berbeda menyebabkan kondisi atau kebutuhan akan metode yang dinilai paling efektif berbeda pula.

5.6.2. Persepsi Auditor Internal Bank Lebih Baik dari Akuntan Pendidik mengenai Efektivitas Metode Pendeteksian dan Pencegahan Tindakan Kecurangan

Hasil analisis *independent t-tes*t dengan pengujian satu arah *(one-tailed test)*, menunjukkan bahwa terdapat hubungan positif antara persepsi internal dan eksternal auditor mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan. Hubungan positif ini dibuktikan dengan adanya perbedaan rata-rata persepsi auditor internal dan eksternal pada uji-t, serta dilihat dari nilai *mean* internal auditor bank yang lebih besar dari akuntan pendidik. Hubungan ini menunjukkan persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan.

Persepsi auditor internal bank lebih baik dari akuntan pendidik dikarenakan responden yang digunakan adalah auditor internal bank yang

bekerja pada industri perbankan. Faktor yang mendasarinya adalah pendidikan dan pengalaman operasional yang spesifik dari auditor internal bank. Hal ini disebabkan karena perbankan sangat intensif dalam melakukan perbaikan terhadap kinerja internal auditornya.

Berdasarkan persepsi dari auditor internal bank (data terlampir); *fraud auditing*, kebijakan yang berkaitan dengan adanya *whistle blowing*, penerapan akuntansi forensik di perusahaan, teknologi perlidungan dengan metode *firewall* dan pelidungan *password* atau kata sandi merupakan tiga peringkat pertama dari metode pendeteksian dan pencegahan tindakan kecurangan yang memiliki tingkat efektivitas tertinggi. Sedangkan etika terhadap petugas/pegawai dan tinjauan terhadap kontrak pekerjaan merupakan metode yang memiliki rata-rata efektivitas terendah.

BAB VI
KESIMPULAN
DAN SARAN

5.1. Kesimpulan

Tujuan penelitian ini adalah: (1) untuk mengetahui perangkat lunak yang digunakan pada metode dengan penggunaan komputer yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan; (2) untuk mengetahui adanya metode baru berkaitan dengan penggunaan komputer yang efektif untuk pendeteksian dan pencegahan tindakan kecurangan; (3) menguji secara empiris persepsi yang lebih baik/tepat dari auditor internal bank, untuk mengukur ekfektivitas metode pendeteksian dan pencegahan tindakan kecurangan pada sistem informasi berbantuan komputer

Setelah dilakukan pengolahan data, pengujian dan analisis terhadap hasil penelitian, maka dapat ditarik kesimpulan sebagai jawaban permasalahan dan sekaligus merupakan tujuan yang berhasil dicapai. Adapun kesimpulan dari hasil penelitian ini adalah sebagai berikut:

1. Hasil pengolahan data mengenai pengetahuan responden tentang tindakan kecurangan:
   - Diketahui berbagai macam *software* yang digunakan untuk pendeteksian dan pencegahan tindakan kecurangan.
   - Diperoleh metode baru untuk pendeteksian dan pencegahan tindakan kecurangan dari hasil penelitian ini, yaitu teknologi untuk mendeteksi verifikai tanda tangan dengan menggunakan *Signature Verification System* (SVS).
2. Hasil pengujian mengenai persepsi auditor internal bank lebih baik dari

akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan adalah terdapat perbedaan persepsi di antara kedua kelompok responden tersebut. *Mean* persepsi internal auditor bank lebih besar dari akuntan pendidik sehingga diambil keputusan bahwa persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan.

3. Penelitian ini memiliki keterbatasan:
   a. Tidak terdapat penjelasan mengenai seberapa besar penggunaan metode pendeteksian dan pencegahan tindakan kecurangan dalam perusahaan.
   b. Diperoleh metode baru untuk pendeteksian dan pencegahan tindakan kecurangan dalam penelitian ini, yaitu teknologi untuk mendeteksi verifikasi tanda tangan dengan menggunakan *Signature Verification System* (SVS) namun belum belum diketahui seberapa jauh penggunaan dan efektivitasnya.

5.2. Saran

Terdapat beberapa implikasi maupun saran atas kekurangan dari penelitian ini, yang diuraikan sebagai berikut:

1. Penelitian ini mempunyai implikasi yang luas dimasa yang akan datang, khususnya untuk penelitian yang menemukan adanya metode baru yang efektif mendeteksi dan mencegah tindakan kecurangan.
2. Model penelitian merupakan pengembangan dari penelitian sebelumnya oleh Biestaker, *et. al* (2006) yang hanya secara deskriptif menjelaskan

penggunaan serta efektivitas dari metode pendeteksian dan pencegahan tindakan kecurangan, sehingga perlu ditindaklanjuti dengan diteliti kembali apakah terdapat perbedaan persepsi dari kelompok akuntan yang diteliti. Penelitian ini juga menyarankan untuk penelitian selanjutnya dengan memperluas obyek penelitian dengan memilih responden auditor yang bersertifikasi khusus untuk tindakan kecurangan.

3. Perhatian mengenai pendanaan untuk masalah tindakan kecurangan perlu juga diperhatikan, khususnya industri di luar perbankan.
4. Untuk penelitian selajutnya diharapkan dapat menjelaskan penggunaan metode pendeteksian dan pencegahan tindakan kecurangan dalam perusahaan, sehingga dapat membantu dalam pengambilan kebijakan yang lebih baik.
5. Peneltian selanjutnya diharapkan dapat memberikan masukan mengenai penggunaan dan efektivitas dari metode verifikasi tanda tangan dengan menggunakan *Signature Verification System* (SVS).
6. Berdasarkan hasil analisis persepsi auditor internal bank lebih baik dari akuntan pendidik mengenai efektivitas metode pendeteksian dan pencegahan tindakan kecurangan diharapkan dapat memberikan konstribusi bagi pihak yang terkait. Adanya kebijakan yang mengharuskan adanya pelatihan secara berkala/terus-menerus mengenai tindakan kecurangan, terutama bagi akuntan pendidik.
7. Dari hasil analisis terdapat perbedaan persepsi dari kedua kelompok responden mengenai efektivitas metode pendetesian dan pencegahan tindakan kecurangan. Hasil analisis ini menunjukkan persepsi internal auditor bank yang paling tepat digunakan untuk menilai efektivitas metode

pendeteksian dan pencegahan tindakan kecurangan. *Fraud auditing*, rekonsiliasi laporan keuangan, akuntansi forensik, kebijakan yang berkaitan dengan *whistle blowing*, *data mining* dan metode *firewall* menduduki urutan efektivitas tertinggi. Kebijakan mengenai perlindungan saksi yang berani mengungkap kebenaran, andanya ketentuan imbalan kepada *whistle blowing*, pembekalan ilmu berkaitan dengan *fraud auditing* dan *data mining*; merupakan alternatif yang bisa segera direalisasikan untuk mengurangi tindakan kecurangan.

DAFTAR PUSTAKA

Albrecht, W.S. 1996. “Employee fraud”, *Internal auditor*, Vol.25

Albrecht, W.S. and M.B. Romney. 1986. “A red-flagging management fraud: a validation”, *Advances in Accounting*, Vol. 3

Albrecht W.S, 2002 . *Fraud Examination,* Thomson, South- Western

Amrizal. 2004. *Pencegahan dan Pendeteksian Kecurangan oleh Internal Auditor,*http://muhariefeffendi.files.wordpress.com/2007/11/cegah_deteksi-investigasi-bpkp-go-id.pdf. Diakses tanggal 26 Mei 2008

Andersen, S. 2004, “Despite more rigorous compliance programs, corporate fraud still thrives”, *Corporate Legal Times*, Vol. 33

Apostolou, B., J. Hassell, S. Webber, and G. Sumners. 2001. “The relative importance of management fraud risk factors”, *Behavioral Research in Accounting*, Vol. 13

Bank Indonesia. 2008. *Indonesian Bank Statistics*, Vol.6, No.5, April 2008. http://localhost:4664/cache?event_id=51375&schema_id=8&q=Indonesian+Bank+Statistics&s=NN0gGQcftLig7aCdmU6TuzW4RT8. Diakses tanggal 25 Mei 2008

Berry, L.E. 1983. “Coordinating Total Audit Coverage: Trend and Practices. *The Institote of Internal Auditors Research Foundation.* Vol.24

Bierstaker, J.L., R.G. Brody, C. Pacini. 2006. “Accountants’ perceptions regarding fraud detection and prevention methods” *Managerial Auditing Journal,* Vol. 21

Binhadi. 2005. “Proses IT Bank Mandiri Sesuai Prosedur”, *Forum Ekonomi Bisnis Majalah Tempo tanggal 11 Mei 2005*, http://www.tempointeractive.com/hg/ekbis/2005/05/11/brk. Diakses tanggal 24 Mei 2008

Blocher, E. 1992. *The Role of Analytical Procedures in Detecting Management Fraud*, Institute of Management Accountants, Montvale, N J

Bologna, J. 1993. *Handbook on Corporate Fraud*, Butterworth-Heinemann, Stoneham, MA

Budi, S. 2008. “Internal Auditor dan Dilema Etika*”*. *Ringkasan Penelitian*, http://www.theakuntan.com/riset/internal-auditor-dan-dilema-etika/-31k. Diakses tanggal 24 Mei 2008

Calderon, T.G. and B.P. Green, B.P. 1999. “Signaling fraud by using analytical procedures”, *Ohio CPA Journal*, Vol. 53

Chen, C. and Sennetti, J. 2000. “Fraudulent financial reporting characteristics of the computer industry under a strategic-systems lens”, *Journal of Forensic Accounting*, Vol. 6

Cooper, D.R. and C.W. Emory. 1995. *Business Research Methods*, Fifth Edition, Richard D.Irwin Inc., Chicago

Durtschi, C., W. Hillison and C. Pacini. 2000. “Effective use of Benford’s law in detecting fraud in accounting data”, *Journal of Forensic Accounting*, Vol. 5

Fatchurrochman, A. 2001. “Diskusi KAP Bermasalah”. *Majalah Media Akuntansi-IAI, Jakarta, 2 Mei 2001.* http://agamfat.multiply.com/reviews/item/8. Diakses tanggal 24 Mei 2008

Gerard, G., W. Hillison, and C. Pacini. 2004. “Identity theft: the US legal environment and organisations’ related responsibilities”, *Journal of Financial Crime*, Vol. 12

Ghozali, I. 2002. *Aplikasi Analisis Multivariate dengan Program SPSS*, Edisi Kedua. Badan Penerbit Universitas Diponegoro, Semarang

Gramling, A., and P.M. Myers. 1997. “Practitioners’ and User’s Perceptions of the Benefits Certification of Internal Auditors”. *Accounting Horizons*, Vol. 11

Hackenbrack, K. 1993. “The effect of experience with different sized clients on auditor evaluations of fraudulent financial reporting indicators”, *Auditing: A Journal of Practice & Theory*, Vol. 12

Hall, J.A., and T. Singleton. 2004. *Audit Teknologi Informasi dan Assurance,* Edisi Bahasa Indonesia. Penerbit Salemba Empat, Jakarta

Holtfreter, K. 2004. “Fraud in US organisations: an examination of control mechanisms”, *Journal of Financial Crime*, Vol. 12

Hylas, R.E., and R. Ashton. 1982. “Audit detection of financial statement errors”, *The Accounting Review*, Vol. 57

Kaminski, K., and T.S. Wetzel. 2004. “Financial ratios and fraud: an exploratory study using chaos theory”, *Journal of Forensic Accounting*, Vol. 5

Lanza, R. 2000. “Using digital analysis to detect fraud”, *Journal of Forensic Accounting*, Vol. 1

Loebbecke, J.K. and JJ. Willingham. 1988, *Review of SEC Accounting and Auditing Enforcement Releases*, Working Paper, University of Utah, Utah

Loebbecke, J.K., M.M. Eining and J.J. Willingham. 1989. “Auditors’ experience with material irregularities: frequency, nature, and detect-ability”, *Auditing: A Journal of Practice & Theory*, Vol. 9

Mahmud, M.D. 1990. *Psikologi Suatu Pengantar*, BPFE, Yogyakarta

Moyes, G. and C.R. Baker. 2003. “Auditors’ beliefs about the fraud detection effectiveness of standard audit procedures”, *Journal of Forensic Accounting*, Vol. 4

Parmono, V.R. 2003. “Deteksi Dini Tindak Kecurangan Dalam Perusahaan”, *Jurnal Administrasi dan Bisnis,* Vol. 3

Pergola, C.W. and P.C. Sprung. 2005. “Developing a genuine anti-fraud environment”, *Risk Management*, Vol. 52

Pincus, K. 1989. “The efficacy of a red flags questionnaire for assessing the possibility of fraud”, *Accounting, Organizations, and Society*, Vol. 14

Rahardjo, B. 2001. *Aspek Teknologi dan Keamanan dalam Internet Banking,* http://www.cert.or.id/~budi/articles/internet-banking-bi-1.pdf. Diakses tanggal 27 Mei 2008

Ratmanto, B., R. Moezwir, O. Prastomiyono dan A. Setyanti. 2008. “Peran SKAI Bank Dalam Rangka Menyiapkan SDM Menyongsong Standar Kompetensi Kerja Nasional Internal Audit Bank”, *Konferensi Nasional Ikatan Auditors Perbankan Indonesia 2007 pada 12 Juli 2007 di Hotel JW Marriot Jakarta*, http://www.zest-eo.com. Diakses pada tanggal 12 Juli 2008

Robins, S.P. 1996. *Perilaku Organisasi: Konsep, Kontroversi, Aplikasi*, Edisi Bahasa Indonesia. PT. Prenhalindo, Jakarta

Rogow, R.B. and Z. Rezaee. 1990. “Governmental Accounting and Auditing: Recent Developments Leading Toward Professional Certification”, *Accounting Horizons*, Vol. 23

Rohadian, A.R. 2008. “Fraud Auditing In Financial Institution (Banking, Etc)”, *Workshop Principles of Fraud Examination pada tanggal 17-19 Desember 2008 di Bali*, http://www.lpauditorinternal.org. Diakses pada 24 Mei 2008

Santosa, P.B. dan Ashari. 2005. *Analisis Statistik dengan Microsoft Excel dan SPSS*, Penerbit Andi, Yogyakarta

Siboro, D.T. 2007. ”Pengaruh Persepsi Auditor yang Bekerja di Kantor Akuntan Publik yang Berafiliasi dan Non-afiliasi terhadap Metode-Metode Pendeteksian dan Pencegahan Kecurangan”. *Tesis Tidak Dipublikasikan.* Magister Sains Akuntansi, Universitas Diponegoro

Sugiono. 2005. *Metode Penelitian Bisnis*, Cetakan Kedelapan. Penerbit Alfabeta, Bandung.

Tugiman, Hiro. 2008. “Tuntutan Perubahan Paradigma Auditor Internal dan Persepsi Pimpinan Organisasi”, *Ikatan Auditors Perbankan Indonesia*, http://www.zest-eo.com. Diakses pada tanggal 12 Juli 2008.

Tunggal, Amin Widjaja. 1992. *Pemeriksaan Kecurangan (Fraud Auditing)*, Cetakan Pertama. Penerbit Rineka Cipta, Jakarta.

Wright, A. and R. Ashton. 1989. “Identifying audit adjustments with attention-directing procedures”, *The Accounting Review*, Vol. 64.

Sawyers, L.B. 2006. Audit Internal Sawyer, Edisi Bahasa Indonesia, Buku 3, Edisi 5. Salemba Empat, Jakarta

Thompson, C. Jr. 1992. ``Fraud'', *Internal Auditor*, August, Vol. 19

Tuanakotta, T.M. 2007. *Akuntansi Forensik dan Audit Investigatif.* LP-FEUI, Jakarta

Tunggal, A W. 1994. *Dasar-Dasar Akuntansi Bank*. Penerbit Rineka Cipta, Jakarta.

Vibiz Consulting. 2008. *Teknologi Manajemen Resiko*, http://*www.vibiznews.com/*1new/column.php?sub=column&id=379&page=risk - 41k. Diakses tanggal 26 Mei 2008

LAMPIRAN I. KUESIONER

Demografi Responden (**Beri tanda √ dalam kotak sesuai jawaban Anda**)

- Jenis Kelamin : Pria ☐ Wanita ☐
- Usia: ……. tahun
- Tingkat pendidikan tertinggi:
  Sarjana Akuntansi ☐ Pasca sarjana ☐
  Selain program pasca sarjana ☐ :**(mohon indentifikasi)**.....
- Lamanya pengalaman sebagai auditor internal/akuntan pendidik: …..tahun
- Bekerja pada Unit SKAI:
  Ya ☐ Tidak ☐
- Bekerja sebagai staf pengajar pada perguruan tinggi:
  Ya ☐ Tidak ☐

***Pertanyaan untuk mengetahui apakah sistem sudah berjalan dengan baik*:(Beri tanda √ dalam kotak**)

1. Apakah pada waktu mengakses data digunakan PIN atau *password*?
   Ya ☐ Tidak ☐
2. Apakah pengakses data terekam/ter-*record*?
   Ya ☐ Tidak ☐
3. Apakah laporan kinerja sistem secara periodik diperiksa?
   Ya ☐ Tidak ☐

Metode pendeteksian dan pencegahan tindakan kecurangan

Tabel I:
Silakan mengindikasikan langkah-langkah yang Anda ambil untuk mengurangi kemungkinan adanya tindakan kecurangan dalam perusahaan anda dan efektivitas yang anda buat atas tiap langkah untuk mencegah atau mendeteksi tindakan kecurangan dari nilai 1 (Sangat tidak efektif) hingga nilai 5 (Sangat efektif).

1 = Sangat tidak efektif
2 = Tidak efektif
3 = Cukup efektif
4 = Efektif
5 = Sangat efektif

Tabel II:
Silakan mengindikasikan teknologi apa yang anda gunakan untuk mengurangi kemungkinan adanya tindakan kecurangan dalam perusahaan dan efektivitas yang anda rasakan dari setiap aplikasi teknologi tersebut untuk mencegah atau mendeteksi tindakan pemalsuan dari nilai 1 (Sangat tidak efektif) hingga nilai 5 (Sangat efektif). Bila teknologi tersebut berbentuk perangkat *software* maka indikasikan nama dari perangkat *software* tersebut dan apakah perangkat tersebut dikembangkan secara internal atau eksternal dalam perusahaan anda?

TABEL I

Metode/prosedur mengenai tindakan kecurangan/*fraud*	**Efektivitas metode pendeteksian & pencegahan *fraud* (Lingkari pada nomor)**				
1. Kode etik perusahaan atau kebijakan etika pada perusahaan.	1	2	3	4	5
2. Tinjauan terhadap pengendalian internal dan peningkatannya.	1	2	3	4	5
3. Pengecekan terhadap referensi pegawai.	1	2	3	4	5
4. Tinjauan terhadap kontrak pekerjaan.	1	2	3	4	5
5. *Fraud auditing* di perusahaan.	1	2	3	4	5
6. Kebijakan untuk melaporkan tindakan kecurangan.	1	2	3	4	5
7. Tinjauan terhadap kerawanan perusahaan atas tindakan kecurangan.	1	2	3	4	5
8. *Hot line service* untuk melaporkan tindakan kecurangan.	1	2	3	4	5
9. Kebijakan yang berkaitan dengan adanya *whistle-blowing.*	1	2	3	4	5
10. Operasional Audit pada perusahaan.	1	2	3	4	5
11. Penerapan akuntan forensik oleh perusahaan.	1	2	3	4	5

12. Adanya pelatihan pencegahan dan pendeteksian tindakan kecurangan.	1	2	3	4	5
13. Adanya pelatihan etika.	1	2	3	4	5
14. Observasi atau pengamatan terhadap peralatan.	1	2	3	4	5
15. Meningkatkan perhatian pada manajemen senior dalam perusahaan.	1	2	3	4	5
16. Kode pemberian sanksi terhadap pemasok/rekanan.	1	2	3	4	5
17. Meningkatkan peranan komite audit.	1	2	3	4	5
18. Dilakukan observasi terhadap korespondensi secara elektronis.	1	2	3	4	5
19. Kebijakan rotasi pegawai.	1	2	3	4	5
20. Departemen sekuritas.	1	2	3	4	5
21. Program bimbingan pegawai.	1	2	3	4	5
22. Tinjauan terhadap dana tunai perusahaan.	1	2	3	4	5
23. Dilakukan observasi persediaan.	1	2	3	4	5
24. Dilakukan rekonsiliasi laporan keuangan.	1	2	3	4	5
25. Etika terhadap petugas/pegawai.	1	2	3	4	5

TABEL II

Penerapan metode yang berkaitan dengan teknologi/perangkat *sotfware*	**Efektivitas teknologi/ metode pendeteksian & pencegahan *fraud* (Lingkari pada nomor)**
26. Teknologi penetapan sampel untuk observasi atau deteksi.	1 2 3 4 5 Nama *software*:
27. *Data mining.*	1 2 3 4 5 Nama *software*:
28. Analisis digital.	1 2 3 4 5 Nama *software*:
29. Teknologi untuk audit berkelanjutan.	1 2 3 4 5 Nama *software*:
30. Teknologi untuk menghitung rasio keuangan.	1 2 3 4 5 Nama *software*:
31. Teknologi perlindungan terhadap virus.	1 2 3 4 5 Nama *software*:
32. Perlindungan *password* atau kata kunci.	1 2 3 4 5 Nama *software*:
33. Teknologi perlindungan dengan metode *firewal.l*	1 2 3 4 5 Nama *software*:
34. Teknologi untuk menyaring perangkat *software.*	1 2 3 4 5 Nama *software*:

Lainnya: Bila ada, silakan identifikasi aplikasi audit lainya yang dilengkapi dengan perangkat *software*:…….....

LAMPIRAN II
CROSSTAB

Crosstab

		10 BANK UMUM DENGAN ASET TERBESAR										TOTAL
		1	2	3	4	5	6	7	8	9	10	
AIB	SAH	20	14	8	19	0	0	0	0	0	0	61
		11.4%	8.0%	4.5%	10.8%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	34.7%
	TIDAK SAH	7	12	6	12	0	0	0	0	0	0	37
		4.0%	6.8%	3.4%	6.8%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	21.0%
	TIDAK KEMBALI	10	9	4	13	12	4	3	11	2	10	78
		5.7%	5.1%	2.3%	7.4%	6.8%	2.3%	1.7%	6.3%	1.1%	5.7%	44.3%
TOTAL		37	35	18	44	12	4	3	11	2	10	176
		21.0%	19.9%	10.2%	25.0%	6.8%	2.3%	1.7%	6.3%	1.1%	5.7%	100.0%

Crosstab

		PERGURUAN TINGGI PENYELENGGARA PROGDI AKUNTANSI																					TOTAL
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
AP	SAH	12	0	9	9	8	0	8	8	7	0	3	0	0	0	0	0	0	0	0	0	0	0	64
		6.8%	0.0%	5.1%	5.1%	4.5%	0.0%	4.5%	4.5%	4.0%	0.0%	1.7%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	36.4%
	TIDAK SAH	0	0	2	0	2	0	1	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	9
		0.0%	0.0%	1.1%	0.0%	1.1%	0.0%	0.6%	1.1%	1.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	5.1%
	TIDAK KEMBALI	8	15	4	6	5	10	1	0	1	5	2	5	5	5	5	5	5	4	3	3	3	3	103
		4.5%	8.5%	2.3%	3.4%	2.8%	5.7%	0.6%	0.0%	0.6%	2.8%	1.1%	2.8%	2.8%	2.8%	2.8%	2.8%	2.8%	2.3%	1.7%	1.7%	1.7%	1.7%	58.5%
TOTAL		20	15	15	15	15	10	10	10	10	5	5	5	5	5	5	5	5	4	3	3	3	3	176
		11.4%	8.5%	8.5%	8.5%	8.5%	5.7%	5.7%	5.7%	5.7%	2.8%	2.8%	2.8%	2.8%	2.8%	2.8%	2.8%	2.8%	2.3%	1.7%	1.7%	1.7%	1.7%	100.0%

LAMPIRAN III. TABULASI DATA

No	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26	X27	X28	X29	X30	X31	X32	X33	X34	Var t
1	4	4	5	4	5	4	4	4	4	4	5	4	4	4	4	4	4	4	3	4	5	4	4	4	2	4	4	5	4	4	5	4	4	4	X1
2	3	5	2	3	5	2	5	5	5	5	4	3	3	4	5	5	5	3	4	4	4	5	3	5	2	5	5	5	5	3	5	5	5	5	X1
3	5	5	4	3	5	5	5	5	5	5	5	5	5	5	5	5	4	1	3	4	3	3	4	5	4	5	5	5	5	3	5	5	5	5	X1
4	4	4	5	4	5	4	4	4	5	4	4	5	4	5	5	4	5	4	4	2	4	5	2	5	2	4	5	4	5	4	5	5	5	5	X1
5	5	3	3	3	4	3	3	3	4	5	4	4	4	3	4	5	5	3	3	2	3	5	2	5	4	5	5	5	5	5	5	5	5	5	X1
6	5	5	4	2	5	1	4	2	5	5	5	5	5	4	5	5	5	3	3	4	4	3	4	5	2	5	5	5	5	4	5	4	5	4	X1
7	3	5	4	4	5	4	2	3	5	5	5	3	4	5	2	5	3	4	3	3	2	4	3	5	3	5	4	5	5	5	4	5	4	5	X1
8	5	4	5	3	5	5	4	4	4	4	5	5	4	5	5	4	5	3	4	5	4	3	4	4	4	4	5	5	4	4	5	5	5	5	X1
9	5	5	3	3	5	2	4	4	5	5	5	5	4	4	4	5	5	4	3	2	2	3	2	5	3	3	5	4	5	5	5	5	5	5	X1
10	4	3	4	4	5	4	3	3	5	5	5	4	5	5	3	5	4	2	4	3	4	4	3	5	3	5	5	5	5	4	4	5	4	4	X1
11	5	5	2	3	5	4	5	4	5	5	5	5	3	1	5	5	5	3	4	3	3	5	3	5	4	5	5	5	5	4	5	5	5	5	X1
12	5	5	3	3	5	3	1	3	3	4	3	5	5	3	5	4	5	4	4	4	3	4	4	5	3	5	5	5	5	4	5	4	5	5	X1
13	4	5	4	4	3	4	3	1	5	5	5	3	4	5	4	5	5	2	3	2	2	4	3	4	3	4	4	5	5	3	5	5	5	5	X1
14	3	4	5	3	5	2	4	3	5	5	4	5	4	4	3	5	3	4	4	4	4	1	4	5	4	5	5	5	5	4	4	5	4	4	X1
15	4	5	3	4	5	3	3	4	5	5	5	4	3	5	5	5	5	3	3	3	3	4	2	5	3	3	5	5	5	5	5	5	5	5	X1
16	1	5	4	3	5	4	4	4	4	5	5	5	5	3	2	5	5	3	4	4	3	4	4	5	2	5	5	4	4	4	3	5	5	3	X1
17	4	5	3	2	5	4	2	3	5	4	5	5	2	5	5	4	4	4	3	2	4	2	4	5	4	4	5	5	5	5	5	4	5	5	X1
18	5	3	4	4	5	4	4	2	5	5	5	5	4	4	4	5	2	3	2	2	2	4	3	5	3	5	2	2	5	4	5	5	3	4	X1
19	4	5	4	3	5	1	4	3	5	2	5	3	5	4	5	5	5	4	4	4	4	3	4	4	3	5	5	5	5	3	5	2	5	5	X1
20	2	4	4	3	4	3	3	4	5	5	5	4	5	3	3	5	5	3	4	3	3	4	4	5	4	2	4	5	5	2	5	5	4	5	X1
21	5	5	5	4	5	4	4	3	5	4	5	5	4	4	5	5	5	2	4	4	2	4	3	5	1	3	5	5	4	4	5	4	5	4	X1
22	4	5	4	3	5	4	3	4	5	5	5	5	3	2	4	4	4	4	3	3	4	3	4	5	3	5	5	4	5	1	5	5	5	5	X1
23	4	2	5	4	5	2	4	3	5	3	5	5	5	5	5	5	5	3	3	4	3	3	3	5	4	4	3	5	5	3	3	4	5	3	X1
24	1	4	3	2	5	4	4	2	5	5	5	4	4	3	5	5	5	4	3	3	3	4	3	4	3	5	5	5	5	4	5	5	3	4	X1
25	2	5	4	3	5	3	3	3	5	4	5	5	5	5	3	5	5	2	4	4	4	2	2	5	4	5	5	3	5	5	5	3	5	5	X1
26	3	5	2	4	3	4	3	2	5	5	5	5	4	4	4	5	5	3	2	3	3	4	4	2	3	3	5	5	3	4	5	5	5	5	X1
27	4	5	3	3	5	4	4	4	5	5	5	3	1	5	5	4	4	4	5	4	4	5	4	5	4	5	4	5	5	3	5	4	5	4	X1
28	4	4	4	3	5	3	4	3	5	4	5	5	4	3	5	2	5	2	2	3	2	4	3	5	2	4	5	4	4	2	4	5	5	5	X1
29	5	5	3	4	5	3	4	2	5	3	5	4	3	4	5	5	5	4	2	4	2	3	4	5	4	5	5	5	5	4	5	5	5	5	X1
30	3	2	1	3	5	4	3	1	3	5	5	5	5	5	4	5	5	4	3	3	4	4	3	4	3	2	3	2	5	3	5	4	5	5	X1
31	5	3	4	2	5	4	4	5	5	5	5	5	4	4	3	5	5	3	3	3	3	3	3	3	4	5	5	5	2	5	5	5	5	2	X1
32	4	4	3	4	5	3	3	4	5	4	5	5	5	1	1	5	5	4	3	4	4	4	4	5	3	4	5	5	5	4	5	5	5	4	X1
33	3	1	4	3	5	4	4	3	5	5	5	2	4	4	2	3	4	3	3	4	3	3	4	5	3	1	5	5	4	3	5	5	4	5	X1
34	4	5	3	4	5	3	4	5	5	5	4	4	3	4	4	5	5	4	4	4	4	4	4	5	4	5	4	4	5	3	5	4	5	5	X1
35	2	5	4	1	5	4	4	4	5	5	5	5	5	5	5	5	5	3	3	4	4	5	3	5	3	3	5	5	5	4	3	5	3	5	X1
36	4	4	4	4	5	3	2	3	5	5	5	5	4	3	4	4	5	4	3	3	4	4	4	5	4	5	5	5	5	3	5	5	5	5	X1
37	3	5	4	3	5	4	3	4	5	4	5	5	2	2	5	5	5	4	3	4	3	4	2	5	3	4	5	5	5	4	5	3	5	5	X1
38	5	5	5	2	5	4	4	4	3	5	5	4	3	5	5	5	5	3	2	3	2	5	3	4	4	4	5	4	3	4	5	5	5	5	X1
39	3	4	3	4	5	3	4	3	5	5	3	5	5	4	3	5	5	4	4	4	4	3	4	5	3	5	5	5	5	3	4	4	5	5	X1
40	4	5	4	2	3	2	3	2	5	3	5	5	4	3	4	5	5	2	3	3	4	4	4	5	4	5	5	3	5	4	5	5	5	5	X1
41	4	5	3	3	5	4	4	4	4	5	5	5	2	4	5	5	5	3	4	1	3	4	4	5	3	3	5	5	5	4	5	5	5	5	X1
42	3	4	4	2	5	4	2	3	5	5	5	5	4	5	4	3	4	2	3	3	4	5	3	5	3	5	5	5	4	4	5	5	5	5	X1
43	5	5	5	3	5	3	3	4	5	5	5	5	5	4	5	5	5	3	2	4	3	4	4	5	2	4	5	5	5	2	4	5	3	3	X1
44	4	5	3	2	5	4	4	3	5	5	3	4	3	2	4	5	5	4	2	2	3	2	4	5	3	4	4	4	5	4	5	5	5	5	X1
45	3	4	4	2	5	3	4	4	5	3	5	5	4	5	5	5	4	3	3	3	4	3	3	5	2	3	5	5	5	3	3	3	5	2	X1
46	4	5	4	3	5	4	4	3	3	5	5	4	5	4	4	5	4	3	2	3	3	4	4	5	2	4	5	3	5	4	5	5	5	5	X1
47	5	4	5	3	4	2	2	4	4	5	5	2	5	5	5	4	4	3	3	5	4	5	4	4	3	4	5	3	5	4	4	5	4	5	X1
48	3	5	3	2	5	3	5	5	5	4	4	5	4	3	4	4	4	3	3	3	4	2	3	5	2	5	3	2	4	2	5	4	4	4	X1
49	2	3	2	3	4	5	3	3	4	2	5	4	2	2	4	5	3	4	3	2	2	3	2	4	3	2	4	5	3	4	3	3	4	4	X1
50	5	4	3	4	5	3	3	3	5	5	3	5	4	1	1	4	4	3	3	3	3	4	3	3	1	3	4	4	4	5	5	4	2	4	X1
51	1	2	5	3	4	3	3	3	4	4	4	4	5	5	5	3	5	4	4	4	4	2	3	4	3	5	5	5	3	3	4	3	5	5	X1
52	5	5	2	2	3	4	5	3	4	4	5	3	4	4	2	4	2	3	3	2	4	5	4	3	3	1	4	4	5	5	4	5	4	3	X1
53	4	4	3	3	5	5	4	3	5	3	4	4	3	3	5	4	4	2	3	4	4	3	5	5	3	4	3	4	4	2	5	3	5	2	X1
54	5	3	5	3	4	4	3	3	4	4	4	5	1	2	4	2	5	3	3	3	3	5	4	4	2	4	4	5	4	3	4	4	4	4	X1
55	3	5	2	1	4	3	3	3	4	5	5	4	5	5	3	4	4	3	3	4	2	4	3	4	3	5	5	3	5	4	5	4	5	3	X1
56	4	4	3	3	5	2	2	4	4	4	4	2	2	3	2	3	4	4	3	2	3	3	3	4	3	4	4	5	4	5	3	5	4	4	X1
57	2	5	4	2	5	5	5	4	4	2	4	4	4	1	5	4	4	3	3	4	1	4	3	5	3	3	4	4	4	3	4	2	3	4	X1
58	3	4	3	3	4	3	3	3	4	4	5	4	3	5	4	4	5	3	3	3	4	5	4	4	4	5	2	2	4	2	4	2	4	5	X1
59	3	2	5	4	5	2	3	2	5	5	4	2	4	3	1	4	3	4	4	4	3	3	3	2	3	2	4	3	2	5	5	4	5	2	X1
60	5	4	3	3	4	3	3	3	4	3	2	5	5	5	4	5	4	3	3	3	4	5	2	4	4	5	5	5	4	3	2	5	4	5	X1
61	1	5	2	3	2	3	3	3	4	4	4	4	1	4	5	4	4	3	3	3	4	2	3	4	3	4	4	4	4	4	4	4	4	4	X1
62	3	4	4	2	5	4	3	2	5	4	3	4	3	4	4	5	3	3	4	4	3	4	5	3	3	3	5	4	4	5	5	3	5	4	X2
63	4	3	3	4	5	3	4	3	4	3	4	3	4	4	3	3	4	2	3	3	2	3	3	4	3	4	4	4	4	3	5	5	4	4	X2
64	5	5	5	3	4	5	3	3	3	3	5	4	2	3	4	4	5	3	4	2	3	3	2	5	2	2	5	4	3	2	3	4	5	3	X2
65	3	3	4	3	5	3	3	3	5	4	4	4	3	3	3	4	4	3	3	5	5	5	3	5	3	4	3	4	4	3	5	4	3	4	X2
66	4	4	3	3	4	2	3	3	4	4	5	2	5	1	3	3	4	3	3	4	3	2	4	4	2	4	4	3	5	4	4	5	4	5	X2
67	4	5	3	2	5	3	3	3	4	2	4	4	4	3	4	4	3	2	3	3	3	3	3	3	3	3	5	2	5	3	5	4	5	3	X2
68	4	4	3	3	4	3	2	4	5	4	5	4	2	4	2	4	3	3	3	2	3	4	3	3	3	5	3	4	4	4	5	3	3	4	X2
69	4	3	4	2	3	4	5	2	3	3	5	3	3	3	3	3	4	3	3	3	2	2	3	4	3	3	5	4	3	3	5	4	4	4	X2
70	2	4	3	3	5	3	3	3	5	4	3	3	3	2	4	5	4	4	3	3	3	3	2	4	3	5	4	3	4	3	4	4	4	3	X2
71	3	1	3	3	5	3	3	4	5	3	4	4	3	3	5	4	4	3	3	1	4	3	4	3	3	5	3	4	4	4	5	4	5	4	X2
72	3	4	3	3	4	2	3	4	4	4	4	4	4	2	2	5	4	3	3	3	3	4	3	5	3	4	3	3	3	3	3	4	5	3	X2
73	3	4	4	1	5	3	4	3	4	3	5	3	3	4	4	4	5	3	3	3	2	3	3	4	3	3	4	4	3	4	4	3	4	4	X2
74	4	2	3	3	3	4	4	4	3	4	5	5	4	3	3	3	5	4	3	3	2	3	3	5	2	4	4	3	4	2	5	3	5	4	X2
75	3	3	1	3	5	3	3	4	5	5	5	4	3	3	5	4	4	3	3	3	3	4	4	4	3	1	5	5	5	4	4	4	3	2	X2
76	2	4	4	3	3	4	3	3	3	3	4	3	3	4	4	4	4	4	3	3	3	3	4	4	3	3	4	3	5	3	3	5	4	5	X2
77	3	4	3	3	5	3	4	3	5	4	3	4	4	1	3	4	3	4	2	3	3	4	3	4	3	4	4	4	4	3	5	4	5	4	X2
78	3	5	3	2	5	5	5	3	5	5	5	5	5	5	5	5	3	5	3	5	5	3	5	5	3	5	5	5	5	3	3	3	3	5	X2
79	5	2	5	3	3	2	3	4	5	3	3	3	3	3	2	3	5	4	3	3	4	3	3	2	2	2	3	3	3	5	5	3	3	3	X2
80	3	3	3	3	5	3	4	5	3	3	3	2	3	3	3	5	4	2	3	3	2	3	2	5	5	2	3	3	5	3	3	3	3	2	X2
81	5	2	5	2	5	4	2	2	5	5	5	3	5	3	4	3	5	5	3	3	5	5	5	2	2	3	5	3	3	3	4	3	5	5	X2
82	3	5	3	3	3	3	2	3	3	3	3	5	3	5	3	3	2	3	3	5	3	3	3	3	3	5	3	5	3	3	5	3	5	3	X2
83	3	3	3	3	5	5	3	4	3	3	5	3	2	3	3	5	3	3	3	3	1	5	4	5	4	3	3	3	5	5	3	3	4	3	X2
84	5	3	2	2	3	3	5	2	3	3	3	3	1	3	5	3	5	4	2	2	2	2	3	3	3	2	5	3	3	3	2	3	5	5	X2
85	3	5	3	3	3	3	3	2	5	5	3	2	5	3	3	3	3	3	3	3	4	3	3	3	2	3	3	3	3	3	5	3	5	2	X2
86	3	3	3	2	5	2	2	3	3	3	5	3	3	5	4	3	4	3	3	3	3	2	3	3	4	3	3	3	3	3	3	3	2	3	X2
87	5	3	5	3	3	3	2	5	3	3	3	5	3	4	1	5	3	3	2	5	2	5	3	5	3	5	3	5	5	5	5	5	5	5	X2
88	3	3	3	3	5	5	5	3	5	2	3	3	3	2	5	3	5	2	3	4	3	4	4	4	3	4	5	3	3	2	4	4	3	3	X2
89	3	5	4	2	3	3	3	3	4	5	5	3	5	5	3	2	2	4	2	3	1	3	2	2	3	4	3	2	2	3	5	2	5	2	X2
90	5	2	2	3	5	3	2	4	3	3	4	3	3	3	2	5	3	3	3	2	2	5	3	5	4	3	3	2	3	3	5	5	5	3	X2
91	3	1	3	3	5	4	4	4	5	4	5	2	4	4	5	3	5	3	3	3	3	3	3	4	3	4	5	5	5	1	3	4	3	2	X2
92	3	5	4	3	4	3	2	2	3	3	5	3	3	3	4	2	4	3	3	3	2	4	5	3	2	5	3	3	3	3	3	5	5	5	X2
93	5	3	3	3	5	3	5	3	3	2	3	5	5	5	3	3	3	2	4	3	4	5	3	5	4	3	3	2	3	2	4	2	3	3	X2
94	4	2	5	2	3	5	2	2	3	5	3	3	2	3	5	5	5	4	3	4	3	1	2	4	3	2	5	5	5	5	3	5	4	3	X2
95	3	3	2	3	5	3	2	4	5	3	2	3	3	4	3	3	2	2	3	3	3	2	2	3	3	3	4	3	3	3	3	5	5	2	X2
96	3	5	3	3	5	3	5	3	4	5	3	2	5	5	2	4	4	3	4	2	2	3	3	4	3	3	3	1	3	4	5	3	3	5	X2
97	5	3	4	3	5	3	3	5	5	3	5	3	3	3	4	3	3	2	2	1	3	4	5	4	4	5	5	2	5	3	3	5	5	3	X2
98	2	2	3	3	4	2	4	3	5	2	2	5	3	3	5	5	5	1	3	4	2	3	2	2	3	1	5	5	2	2	3	2	3	4	X2
99	2	5	5	2	4	3	3	2	3	5	3	3	4	5	3	4	3	2	3	3	4	2	3	5	2	2	3	3	3	4	3	3	5	2	X2
100	4	4	3	3	3	3	5	3	5	3	4	2	5	3	4	3	4	4	4	2	3	5	3	3	3	3	5	4	4	5	3	5	5	5	X2
101	3	3	2	3	3	4	3	4	4	3	5	3	2	2	3	3	5	3	3	3	2	3	3	5	4	3	4	3	3	2	3	3	3	3	X2
102	3	2	3	4	5	3	3	3	5	3	3	5	3	1	5	5	3	3	4	4	4	3	2	4	3	5	2	5	5	3	3	4	3	3	X2
103	2	5	4	3	3	3	3	4	5	5	4	3	5	3	2	3	2	3	3	3	3	4	4	3	1	3	5	3	3	4	5	3	5	2	X2
104	3	3	3	2	3	4	5	3	3	3	5	3	3	3	3	4	5	2	2	2	2	3	3	5	2	1	5	3	5	5	4	5	3	5	X2
105	3	1	5	3	5	3	3	4	3	3	3	2	4	5	3	3	3	3	3	1	2	2	3	2	3	2	4	5	4	3	3	3	3	3	X2
106	2	2	3	2	3	5	3	3	5	5	5	5	2	3	5	5	5	4	4	2	4	5	4	5	2	3	5	3	3	2	5	3	5	4	X2
107	4	5	2	3	4	3	4	3	5	3	3	3	5	2	3	2	5	2	3	3	5	3	3	3	3	5	3	3	5	3	3	5	4	3	X2
108	3	3	3	1	2	3	3	4	4	2	5	2	1	3	4	3	4	3	2	3	2	3	3	4	3	4	3	3	3	3	3	2	2	3	X2
109	2	2	2	3	3	3	3	2	3	4	3	5	3	4	3	5	2	2	3	3	1	3	4	5	2	3	5	5	4	5	5	4	5	5	X2
110	3	5	4	3	5	3	4	3	5	3	5	1	2	3	3	3	5	1	3	2	2	4	3	3	3	2	5	3	3	3	5	5	3	3	X2
111	3	3	3	3	4	3	3	2	5	3	5	3	3	2	5	4	3	3	3	4	3	3	3	5	2	3	2	2	5	2	5	3	5	3	X2
112	5	3	5	2	5	4	3	2	3	5	3	3	5	4	3	3	3	4	3	2	3	3	4	3	3	5	3	5	4	3	3	4	3	3	X2
113	3	5	3	3	3	3	3	3	3	1	4	3	3	3	3	5	3	2	3	3	2	3	3	3	2	3	3	3	2	4	3	5	3	3	X2
114	3	3	3	2	5	3	3	2	5	3	3	5	3	2	2	2	5	3	2	2	3	4	2	5	3	4	4	3	5	3	5	3	5	5	X2
115	2	3	2	3	2	1	4	3	5	2	3	3	2	3	3	4	3	2	3	2	4	3	3	3	2	3	5	3	5	3	2	3	3	3	X2
116	4	3	3	1	3	2	3	3	3	5	5	1	4	3	3	5	3	3	4	1	3	2	3	3	1	3	4	5	4	5	5	4	3	5	X2
117	3	4	3	3	5	3	2	2	3	3	3	3	3	2	2	3	3	1	3	2	3	3	3	5	3	2	3	3	2	3	3	2	3	3	X2
118	3	3	4	3	3	3	3	3	3	3	3	3	3	4	2	4	3	3	4	3	3	4	2	3	2	4	5	2	5	4	5	4	3	3	X2
119	3	3	5	3	3	3	3	3	4	4	2	5	3	5	3	5	3	2	3	2	3	3	3	3	3	3	2	4	5	3	5	5	3	5	X2
120	4	3	3	4	5	3	2	3	3	2	3	3	4	3	1	2	5	3	3	4	3	5	3	5	3	5	5	3	4	2	2	3	4	3	X2
121	3	4	1	3	3	2	3	4	3	2	4	5	3	2	3	5	3	2	4	3	3	3	3	5	2	3	3	3	2	4	3	2	5	3	X2
122	2	3	3	3	5	3	3	3	3	3	5	5	2	1	3	3	5	3	3	2	3	2	3	3	1	5	2	3	5	3	5	5	3	3	X2

LAMPIRAN IV
HASIL PENGUJIAN ASUMSI KLASIK

Output SPSS untuk Uji Validitas

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
x1	121.7377	151.038	.250	.825
x2	121.4508	148.134	.331	.822
x3	121.8033	152.754	.203	.826
x4	122.3852	155.644	.139	.827
x5	120.8852	149.226	.397	.820
x6	121.9590	154.106	.172	.827
x7	121.8852	154.846	.137	.828
x8	122.0328	154.974	.139	.828
x9	120.9590	149.891	.393	.821
x10	121.3607	144.629	.513	.816
x11	121.0082	149.529	.369	.821
x12	121.4098	146.079	.433	.818
x13	121.6803	150.104	.272	.824
x14	121.7623	150.480	.237	.826
x15	121.5738	147.850	.340	.822
x16	121.1557	148.298	.411	.820
x17	121.1475	149.317	.368	.821
x18	122.1967	153.366	.230	.825
x19	122.1475	155.714	.169	.826
x20	122.1721	151.549	.280	.824
x21	122.1639	151.461	.290	.823
x22	121.7459	151.315	.266	.824
x23	121.9918	153.215	.256	.824
x24	121.0738	147.953	.428	.819
x25	122.3443	154.773	.170	.827
x26	121.5246	146.152	.400	.820
x27	121.0656	147.830	.432	.819
x28	121.3443	145.566	.465	.817
x29	121.0984	146.403	.493	.817
x30	121.7705	155.120	.110	.829
x31	121.2131	147.905	.411	.820
x32	121.0164	149.471	.364	.821
x33	121.0082	149.281	.389	.820
x34	121.3115	145.340	.490	.817

Output SPSS untuk Uji Reliabilitas

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.827	.823	34

Output SPSS untuk Uji Normalitas

One-Sample Kolmogorov-Smirnov Test

		persp
N		122
Normal Parameters[a,b]	Mean	3.6839
	Std. Deviation	.37050
Most Extreme Differences	Absolute	.106
	Positive	.091
	Negative	-.106
Kolmogorov-Smirnov Z		1.176
Asymp. Sig. (2-tailed)		.126

a. Test distribution is Normal.

b. Calculated from data.

LAMPIRAN V
HASIL PENGUJIAN HIPOTESIS

Output SPSS untuk Uji-t

Group Statistics

	jenis	N	Mean	Std. Deviation	Std. Error Mean
persp	AIB	61	3.9581	.25229	.03230
	AP	61	3.4098	.24578	.03147

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
persp	Equal variances assumed	.453	.502	12.156	120	.000	.54822	.04510	.45893	.63750
	Equal variances not assumed			12.156	119.918	.000	.54822	.04510	.45893	.63751

LAMPIRAN VI
EFEKTIVITAS METODE PENDETEKSIAN DAN PENCEGAHAN TINDAKAN KECURANGAN (PERSEPSI INTERNAL AUDITOR BANK)

Metode Pendeteksian dan Pencegahan Tindakan Kecurangan	Efektivitas Metode	*Rangking*
1. Kode etik perusahaan atau kebijakan etika.	3.7049	15
2. Tinjauan terhadap pengendalian internal dan peningkatannya.	4.2459	11
3. Mengecek referensi pegawai.	3.6066	17
4. Tinjauan terhadap kontrak pekerjaan.	3.0164	27
5. *Fraud auditing.*	4.6721	1
6. Kebijakan untuk melaporkan tindakan kecurangan.	3.3934	19
7. Tinjauan atas kerawanan perusahaan atas tindakan kecurangan.	3.4918	18
8. *Hot line service* untuk melaporkan tindakan kecurangan.	3.3115	21
9. Kebijakan yang berkaitan dengan adanya *whistle-blowing*.	4.6066	2
10. Operasional audit.	4.3770	9
11. Penerapan akuntansi forensik oleh perusahaan.	4.6066	2
12. Pelatihan pencegahan dan pendeteksian tindakan kecurangan.	4.3115	10
13. Pelatihan etika.	3.8361	13
14. Observasi atau pengamatan terhadap peralatan.	3.7869	14
15. Meningkatkan perhatian pada manajemen senior dalam perusahaan.	4.0164	12
16. Kode pemberian sanksi terhadap pemasok/rekanan.	4.4754	6
17. Meningkatkan peranan komite audit	4.4590	7
18. Observasi terhadap korespondensi secara elektronis.	3.2131	24
19. Kebijakan rotasi pegawai.	3.1803	25
20. Departemen sekuritas.	3.2787	23
21. Program bimbingan pegawai.	3.2951	22
22. Tinjauan terhadap dana tunai perusahaan.	3.7049	15
23. Observasi persediaan.	3.3607	20
24. Rekonsiliasi laporan keuangan.	4.5410	3
25. Etika terhadap petugas/pegawai.	3.0492	26
26. Teknologi penetapan sampel untuk observasi atau deteksi.	4.0820	11
27. *Data mining*	4.5246	4
28. Analisis digital.	4.3934	8
29. Teknologi untuk audit berkelanjutan.	4.5082	5
30. Teknologi untuk menghitung rasio keuangan	3.6721	16
31. Teknologi perlindungan terhadap virus.	4.3934	7
32. Perlindungan *password* atau kata sandi.	4.5410	3
33. Teknologi perlindungan dengan metode *firewall*.	4.5410	3
34. Teknologi untuk menyaring perangkat *software*.	4.3770	9

Sumber: Data primer yang diolah

LAMPIRAN VII
NILAI TABEL

Tabel t dan r (signifikansi 5%)

df	Tabel t one tail	Tabel t two tail	Tabel r one tail	Tabel r two tail
1	6.3138	12.7062	0.9877	0.9969
2	2.9200	4.3027	0.9000	0.9500
3	2.3534	3.1824	0.8054	0.8783
4	2.1318	2.7764	0.7293	0.8114
5	2.0150	2.5706	0.6694	0.7545
6	1.9432	2.4469	0.6215	0.7067
7	1.8946	2.3646	0.5822	0.6664
8	1.8595	2.3060	0.5494	0.6319
9	1.8331	2.2622	0.5214	0.6021
10	1.8125	2.2281	0.4973	0.5760
11	1.7959	2.2010	0.4762	0.5529
12	1.7823	2.1788	0.4575	0.5324
13	1.7709	2.1604	0.4409	0.5140
14	1.7613	2.1448	0.4259	0.4973
15	1.7531	2.1314	0.4124	0.4821
16	1.7459	2.1199	0.4000	0.4683
17	1.7396	2.1098	0.3887	0.4555
18	1.7341	2.1009	0.3783	0.4438
19	1.7291	2.0930	0.3687	0.4329
20	1.7247	2.0860	0.3598	0.4227
21	1.7207	2.0796	0.3515	0.4132
22	1.7171	2.0739	0.3438	0.4044
23	1.7139	2.0687	0.3365	0.3961
24	1.7109	2.0639	0.3297	0.3882
25	1.7081	2.0595	0.3233	0.3809
26	1.7056	2.0555	0.3172	0.3739
27	1.7033	2.0518	0.3115	0.3673
28	1.7011	2.0484	0.3061	0.3610
29	1.6991	2.0452	0.3009	0.3550
30	1.6973	2.0423	0.2960	0.3494
31	1.6955	2.0395	0.2913	0.3440
32	1.6939	2.0369	0.2869	0.3388
33	1.6924	2.0345	0.2826	0.3338
34	1.6909	2.0322	0.2785	0.3291
35	1.6896	2.0301	0.2746	0.3246
36	1.6883	2.0281	0.2709	0.3202
37	1.6871	2.0262	0.2673	0.3160
38	1.6860	2.0244	0.2638	0.3120
39	1.6849	2.0227	0.2605	0.3081
40	1.6839	2.0211	0.2573	0.3044
41	1.6829	2.0195	0.2542	0.3008
42	1.6820	2.0181	0.2512	0.2973
43	1.6811	2.0167	0.2483	0.2940
44	1.6802	2.0154	0.2455	0.2907
45	1.6794	2.0141	0.2429	0.2876
46	1.6787	2.0129	0.2403	0.2845
47	1.6779	2.0117	0.2377	0.2816
48	1.6772	2.0106	0.2353	0.2787
49	1.6766	2.0096	0.2329	0.2759
50	1.6759	2.0086	0.2306	0.2732
51	1.6753	2.0076	0.2284	0.2706
52	1.6747	2.0066	0.2262	0.2681
53	1.6741	2.0057	0.2241	0.2656
54	1.6736	2.0049	0.2221	0.2632
55	1.6730	2.0040	0.2201	0.2609
56	1.6725	2.0032	0.2181	0.2586
57	1.6720	2.0025	0.2162	0.2564
58	1.6716	2.0017	0.2144	0.2542
59	1.6711	2.0010	0.2126	0.2521
60	1.6706	2.0003	0.2108	0.2500
61	1.6702	1.9996	0.2091	0.2480
62	1.6698	1.9990	0.2075	0.2461
63	1.6694	1.9983	0.2058	0.2441
64	1.6690	1.9977	0.2042	0.2423
65	1.6686	1.9971	0.2027	0.2404
66	1.6683	1.9966	0.2012	0.2387
67	1.6679	1.9960	0.1997	0.2369
68	1.6676	1.9955	0.1982	0.2352
69	1.6672	1.9949	0.1968	0.2335
70	1.6669	1.9944	0.1954	0.2319
71	1.6666	1.9939	0.1940	0.2303
72	1.6663	1.9935	0.1927	0.2287
73	1.6660	1.9930	0.1914	0.2272

74	1.6657	1.9925	0.1901	0.2257
75	1.6654	1.9921	0.1888	0.2242
76	1.6652	1.9917	0.1876	0.2227
77	1.6649	1.9913	0.1864	0.2213
78	1.6646	1.9909	0.1852	0.2199
79	1.6644	1.9905	0.1841	0.2185
80	1.6641	1.9901	0.1829	0.2172
81	1.6639	1.9897	0.1818	0.2159
82	1.6636	1.9893	0.1807	0.2146
83	1.6634	1.9890	0.1796	0.2133
84	1.6632	1.9886	0.1786	0.2120
85	1.6630	1.9883	0.1775	0.2108
86	1.6628	1.9879	0.1765	0.2096
87	1.6626	1.9876	0.1755	0.2084
88	1.6624	1.9873	0.1745	0.2072
89	1.6622	1.9870	0.1735	0.2061
90	1.6620	1.9867	0.1726	0.2050
91	1.6618	1.9864	0.1716	0.2039
92	1.6616	1.9861	0.1707	0.2028
93	1.6614	1.9858	0.1698	0.2017
94	1.6612	1.9855	0.1689	0.2006
95	1.6611	1.9853	0.1680	0.1996
96	1.6609	1.9850	0.1671	0.1986
97	1.6607	1.9847	0.1663	0.1975
98	1.6606	1.9845	0.1654	0.1966
99	1.6604	1.9842	0.1646	0.1956
100	1.6602	1.9840	0.1638	0.1946
101	1.6601	1.9837	0.1630	0.1937
102	1.6599	1.9835	0.1622	0.1927
103	1.6598	1.9833	0.1614	0.1918
104	1.6596	1.9830	0.1606	0.1909
105	1.6595	1.9828	0.1599	0.1900
106	1.6594	1.9826	0.1591	0.1891
107	1.6592	1.9824	0.1584	0.1882
108	1.6591	1.9822	0.1576	0.1874
109	1.6590	1.9820	0.1569	0.1865
110	1.6588	1.9818	0.1562	0.1857
111	1.6587	1.9816	0.1555	0.1848
112	1.6586	1.9814	0.1548	0.1840
113	1.6585	1.9812	0.1541	0.1832
114	1.6583	1.9810	0.1535	0.1824
115	1.6582	1.9808	0.1528	0.1816
116	1.6581	1.9806	0.1522	0.1809
117	1.6580	1.9804	0.1515	0.1801
118	1.6579	1.9803	0.1509	0.1793
119	1.6578	1.9801	0.1502	0.1786
120	1.6577	1.9799	0.1496	0.1779
121	1.6575	1.9798	0.1490	0.1771
122	1.6574	1.9796	0.1484	0.1764
123	1.6573	1.9794	0.1478	0.1757
124	1.6572	1.9793	0.1472	0.1750
125	1.6571	1.9791	0.1466	0.1743
126	1.6570	1.9790	0.1460	0.1736
127	1.6569	1.9788	0.1455	0.1729
128	1.6568	1.9787	0.1449	0.1723
129	1.6568	1.9785	0.1443	0.1716
130	1.6567	1.9784	0.1438	0.1710
131	1.6566	1.9782	0.1432	0.1703
132	1.6565	1.9781	0.1427	0.1697
133	1.6564	1.9780	0.1422	0.1690
134	1.6563	1.9778	0.1416	0.1684
135	1.6562	1.9777	0.1411	0.1678
136	1.6561	1.9776	0.1406	0.1672
137	1.6561	1.9774	0.1401	0.1666
138	1.6560	1.9773	0.1396	0.1660
139	1.6559	1.9772	0.1391	0.1654
140	1.6558	1.9771	0.1386	0.1648
141	1.6557	1.9769	0.1381	0.1642
142	1.6557	1.9768	0.1376	0.1637
143	1.6556	1.9767	0.1371	0.1631
144	1.6555	1.9765	0.1367	0.1625
145	1.6554	1.9765	0.1362	0.1620
146	1.6554	1.9763	0.1357	0.1614
147	1.6553	1.9762	0.1353	0.1609
148	1.6552	1.9761	0.1348	0.1603
149	1.6551	1.9760	0.1344	0.1598

DAFTAR RIWAYAT HIDUP

Nama Lengkap : Febra Robiyanto, SE, MSi, Akt

Tanggal Lahir/Umur : 19 Februari 1977 / 33 tahun

Tempat Lahir : Semarang

Jenis Kelamin : Laki-laki

Agama : Islam

Status Perkawinan : Kawin

Alamat Rumah : Jl. Bromo V/169-170 Perum Muria Indah Blok E Gondangmanis Bae Kudus

Telp. : (0291) 435282, 08156610959, 08882541892

Pendidikan :

Sekolah Dasar	: SDN Wonodri V Smg	: 1983-1989
SMP	: Maria Mediatrix Smg	: 1989-1992
SMA	: SMAN 1 Smg	: 1992-1995
S1	: FE-Akt UNDIP Smg	: 1995-1999
S2	: Maksi UNDIP Smg	: 2007-2009

Pekerjaan :

Dosen Tetap Universitas Pandanaran Smg	: 1999-2001
Dosen Tetap Universitas Muria Kudus	: 2001- skrg
Pimpinan BJAP	: 2003- skrg

Riwayat Penelitian :

1. Analisis Titik Impas Usaha Penyamakan Kulit Sapi PT. Amor Abadi Kotamadya Dati II Semarang (2003)
2. Sistem Pengendalian Intern Unit Jasa Giro pada Bank Internasional Indonesia Cabang Kudus (2007)
3. Pengaruh Variabel-Variabel Keuangan dan Makro terhadap Risiko Investasi Saham pada Bursa Efek Indonesia (2009).

Demikian Daftar Riwayat dinyatakan dengan sebenar-benarnya.

Kudus, 21 Maret 2009

Yang menyatakan,

Febra Robiyanto, SE, MSi, Akt