AKUNTANSI FORENSIK

Prof. Dr. Edy Sujana, S.E., M.Si., Ak., CA., CFrA.

AKUNTANSI FORENSIK

Prof. Dr. Edy Sujana, S.E., M.Si., Ak., CA., CFrA.

Penerbit Widina

AKUNTANSI FORENSIK

Penulis:
Prof. Dr. Edy Sujana, S.E., M.Si., Ak., CA., CFrA.

Desain Cover:
Septian Maulana

Sumber Ilustrasi:
www.freepik.com

Tata Letak:
Handarini Rohana

Editor:
N. Rismawati

ISBN:
978-623-500-277-4

Cetakan Pertama:
Juli, 2024

PENERBIT:
WIDINA MEDIA UTAMA
Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 360/JBA/2020
Website: www.penerbitwidina.com
Instagram: @penerbitwidina
Telepon (022) 87355370

KATA PENGANTAR

Kecurangan dapat terjadi dimana saja, kapan saja dan oleh siapa saja. Kecurangan dapat menyebabkan kerugian jangka panjang, sehingga diperlukan adanya pengetahuan dan keterampilan khusus untuk dapat menelusuri lebih mendalam terkait kecurangan tersebut. Akuntansi Forensik adalah pengetahuan dan keterampilan yang dapat memberikan pengetahuan untuk mencegah, mendeteksi dan merespon kecurangan yang mungkin terjadi pada organisasi.

Dalam buku Akuntansi Forensik edisi revisi ini, disajikan materi yang berkaitan dengan pendeteksian kecurangan beserta pencegahannya. Edisi ini dilengkapi dengan contoh *Fraud Risk Assesment* pada sebuah organisasi Lembaga Perkreditan Desa. Sebagian buku ini merupakan hasil terjemahan dari buku *Fraud Auditing And Forensic Accounting, Fourth Edision*, karya Tommie W. Singleton dan Aaron J. Singleton yang dikembangkan sesuai pemahaman penulis serta materi disajikan disesuaikan dengan kebutuhan.

Sebagai rasa Syukur penulis mengucapkan terima kasih kehadapan Tuhan yang Maha Esa atas segala Rahmat yang diberikan sehingga buku ini dapat terselesaikan. Ucapan terima kasih kami sampaikan kepada mahasiswa; Meya, Sunarti, Onik, Sukriani, Wira, Sariasih, Fathin dan Teguh yang sudah membantu sehingga proses penyelesaian buku ini bisa tepat pada waktunya. Dan akhir kata kami ucapkan terima kasih kepada semua pihak yang telah memberikan kontribusi dalam penyusunan buku ini. Dan kritik dan saran sangat kami harapkan untuk penyempurnaan buku ini di masa yang akan datang.

DAFTAR ISI

BAB 1
LATAR BELAKANG KECURANGAN AUDIT DAN AKUNTANSI FORENSIK

A. PENGANTAR

Pada dekade pertama abad ke-21, berita dipenuhi dengan laporan tentang kecurangan yang semakin meluas dan biaya yang meningkat bagi ekonomi AS. Hampir semua orang mendengar tentang skandal laporan keuangan perusahaan seperti Enron dan WorldCom, atau penipuan terhadap pemerintah seperti klaim palsu pasca Badai Katrina, serta skema Ponzi besar seperti penipuan Madoff yang mencetak rekor kerugian akibat kecurangan. Banyak orang juga terdampak langsung oleh pencurian identitas. Krisis ekonomi yang dimulai pada tahun 2008 membuat pemulihan dari kerugian tersebut semakin sulit. Lebih buruknya lagi, laporan tentang aktivitas terkait kecurangan terus membawa berita negatif.

Laporan tahun 2007 dari *Federal Bureau of Investigation* (FBI) memperkirakan bahwa penipuan dalam biaya asuransi *non*-kesehatan mencapai lebih dari $40 miliar per tahun, yang mengakibatkan keluarga di AS harus menanggung peningkatan premi sebesar $400 hingga $700 per tahun. Dalam laporan yang sama, FBI memperkirakan bahwa klaim palsu terkait bencana Badai Katrina menghabiskan biaya hingga $6 miliar. Selain itu, FBI melaporkan terjadinya peningkatan sebesar 36% dalam *Suspicious Activity Reports* (SAR) yang diajukan oleh bank pada tahun 2008 jika dibandingkan dengan tahun sebelumnya. Dari jumlah SAR yang diajukan pada tahun 2007, sebesar 7% menunjukkan kerugian finansial tertentu dengan total lebih dari $813 juta. Pada tahun 2008, FBI juga sedang menyelidiki kasus lebih dari $1 miliar dalam penipuan hipotek. Semua fakta ini terjadi sebelum krisis ekonomi dan peningkatan pengawasan terhadap industri hipotek subprime.

Internet Crime Complaint Center (IC3) adalah badan pengawas federal yang dibentuk sebagai hasil kemitraan antara *National White Collar Crime Center* (NW3C) dan FBI. Badan ini berfungsi sebagai pusat untuk menerima, memproses, dan merujuk pengaduan mengenai kejahatan siber yang terus berkembang. Laporan tahunan 2008 menunjukkan peningkatan pengajuan keluhan sebesar 33% jika dibandingkan dengan tahun 2007, yang mencerminkan tren selama dekade tersebut. Total kerugian dari keluhan yang diterima pada tahun 2008 mencapai $265 juta, dengan kerugian rata-rata sebesar $931.000 per keluhan.

BAB 2
PRINSIP-PRINSIP KECURANGAN

A. PENGANTAR

Kecurangan memiliki banyak definisi dan cara penggolongan yang bisa membingungkan. Pemahaman yang tepat tentang definisi dan model ini sangat penting untuk mencegah dan mendeteksi kecurangan. Prinsip kecurangan adalah dasar dari program anti kecurangan yang efektif, atau pencegahan yang efektif dan deteksi dini kecurangan.

Pertama, penting untuk mendefinisikan apa itu kecurangan, baik untuk profesi tertentu maupun untuk organisasi yang membuat program pencegahan kecurangan. Penting juga untuk selalu mengingat kemungkinan adanya kecurangan agar tidak terjebak dalam pemikiran bahwa "*it-can't-happen-here*". Memahami model yang efektif seperti segitiga kecurangan berguna dalam memahami mengapa terjadi kecurangan. Meskipun ada banyak model klasifikasi untuk skema kecurangan, penting untuk memilih satu yang dapat diterapkan secara efektif dalam upaya pencegahan dan deteksi dini. Selain itu, memahami profil pelaku kejahatan kerah putih juga sangat berguna.

B. DEFINISI: APA KECURANGAN?

Kecurangan memiliki arti yang berbeda bagi orang-orang dalam berbagai situasi. Misalnya, kecurangan bisa dianggap sebagai penipuan. Orang mungkin menganggap kecurangan dalam bentuk penipuan internasional (termasuk kebohongan dan penipuan) sebagai lawan dari kebenaran, keadilan, kejujuran, dan kewajaran. Walaupun kecurangan bisa memaksa orang bertindak melawan kepentingan pribadi mereka, kecurangan juga bisa digunakan untuk membela diri atau mempertahankan diri. Terlepas dari alasannya, kecurangan umumnya dianggap buruk dan salah menurut standar perilaku saat ini. Namun, penipuan juga bisa dilakukan untuk tujuan yang baik. Penipu yang bertindak dengan niat baik tidak dipandang seburuk mereka yang motifnya tidak murni. Orang yang bertindak karena keserakahan, cemburu, dendam, atau balas dendam tidak begitu mudah diampuni atau dimaafkan.

Kecurangan juga bisa dikaitkan dengan cedera. Seseorang bisa melukai orang lain secara paksa atau melalui kecurangan. Kekerasan yang menyebabkan cedera fisik tidak diterima oleh masyarakat yang terorganisir dengan baik; namun, menggunakan kecurangan untuk menyebabkan

BAB 3
SKEMA KECURANGAN

A. PENGANTAR

Untuk mencegah kecurangan, mendeteksi kecurangan, atau menyelidiki kecurangan, orang perlu memahami skema kecurangan sebanyak mungkin. Pada Bab 2, berbagai klasifikasi disajikan untuk mengelompokkan kecurangan. Penulis percaya klasifikasi terbaik untuk memahami skema kecurangan adalah yang digunakan oleh *Association of Certified Fraud Examiners* (ACFE). Ada beberapa alasan untuk menyatakan pilihan ini adalah yang terbaik.

Pertama, ACFE muncul sebagai organisasi anti kecurangan utama. Satu-satunya tujuan pendirian ACFE adalah profesi anti kecurangan, sedangkan *American Institute of Certified Public Accountant* (AICPA), *Institute of Internal Auditor* (IIA), dan *Information Systems Audit and Control Association* (ISACA) memiliki tujuan utama yang berbeda. Di sisi lain, terdapat kelompok lain yang memiliki tujuan sama namun tidak ada satu-satunya tujuan untuk melawan kecurangan. Dengan demikian, model ACFE dapat digunakan sebagai standar *de facto* untuk menilai seberapa besar tingkat kejujuran dari profesi yang profesional jika dibandingkan dengan adanya anti kecurangan.

Kedua, klasifikasi dari ACFE telah stabil ketika diterapkan dari waktu ke waktu. Ada 49 bentuk kecurangan yang dilakukan individu telah diklasifikasikan ke dalam pohon kecurangan ACFE dan jumlah itu tidak berubah selama bertahun-tahun. Penipu menemukan cara yang berbeda atau bahkan baru untuk melakukan kecurangan, namun yang paling sering adalah salah satu skema kecurangan kuno yang digunakan oleh pelaku (misalnya, internet dan teknologi lainnya membuka cara baru untuk melakukan beberapa kecurangan yang ada dan sebenarnya tidak menciptakan skema baru).

Ketiga, klasifikasi ACFE memiliki sejumlah skema yang telah terbukti terjadi. Sekitar 20 dari 49 skema yang ada dalam klasifikasi ACFE, lebih dari 80 persen skema kecurangan yang dilakukan. Dengan demikian, studi tentang skema kecurangan yang paling umum memungkinkan seorang auditor forensik untuk mendeteksi atau mencegah sebagian besar skema kecurangan yang menjadi potensial dalam perusahaan. Meskipun sifat ini tidak menjadi *special* dengan penerapan klasifikasi ACFE, namun ada baiknya menunjukkan tujuan untuk memahami analisis skema kecurangan yang sedang berjalan tersebut.

BAB 4
RED FLAG

A. PENGANTAR

Dalam buku ini, istilah "*red flag*" digunakan sebagai sinonim untuk sidik jari penipuan (tanda-tanda penipuan). Ketika terjadi kecurangan, selalu ada jejak atau bukti yang ditinggalkan oleh pelaku, seperti sidik jari di tempat kejadian. *Red flag* mencakup berbagai indikasi, seperti anomali akuntansi, transaksi atau kejadian yang tidak dapat dijelaskan, elemen transaksi yang tidak biasa, dan perubahan atau karakteristik perilaku seseorang. Ini adalah tanda-tanda yang sering dikaitkan dengan penipuan, baik oleh individu maupun kelompok.

Landasan pencegahan dan deteksi kecurangan yang efektif disajikan dalam Bab 1, 2, dan 3. Bab 1 menjelaskan proses penyelidikan kecurangan. Bab 2 memperkenalkan dasar-dasar kecurangan, seperti alasan mengapa kecurangan terjadi (segitiga kecurangan), lingkup kecurangan, aksioma kecurangan, dan profil tipikal penipu. Informasi ini berguna untuk mengembangkan program anti-kecurangan, melakukan pengujian, atau penyelidikan kecurangan. Bab 3 membahas skema kecurangan menggunakan konsep pohon kecurangan, yang sangat penting untuk mendeteksi dan mencegah kecurangan. Seorang auditor kecurangan atau akuntan forensik harus memahami skema kecurangan spesifik dan bagaimana skema tersebut biasanya dilakukan. Semua ini bersatu dalam mempelajari, menganalisis, dan menggunakan *red flag* untuk mencegah dan mendeteksi kecurangan.

Misalnya, pendekatan teori kecurangan dimulai dengan mengidentifikasi skema kecurangan yang paling mungkin terjadi dan bagaimana hal itu bisa dilakukan. Pendekatan ini memerlukan pemahaman mendalam tentang berbagai skema kecurangan dan kemungkinan terjadinya dalam kondisi tertentu, seperti jenis industri, kondisi pengendalian internal, ukuran bisnis dan sebagainya. Untuk membuktikan atau membantah teori tersebut, peneliti kecurangan mencari tanda-tanda (*red flag*) yang menunjukkan terjadinya skema kecurangan tersebut.

Tinjauan analitis yang cermat terhadap pohon kecurangan (skema) dan segitiga kecurangan membantu mengidentifikasi tanda-tanda penipuan yang relevan. Misalnya, dalam skema kecurangan *lapping*, pelaku memanipulasi pembayaran pelanggan dengan menerapkan pembayaran dari satu pelanggan ke akun pelanggan lain yang telah dicuri sebelumnya. Penipu jenis ini tidak dapat mengambil liburan panjang karena skemanya akan terungkap jika ia

BAB 5
PENILAIAN RISIKO KECURANGAN

A. PENGANTAR

Sejak skandal Enron dan kasus kecurangan lainnya, ada fokus besar pada kecurangan, pengendalian internal, dan manajemen risiko kecurangan, termasuk penilaian risiko. *Sarbanes-Oxley Act* (SOX) tahun 2002 meningkatkan perhatian pada masalah ini dan mengintegrasikan prinsip-prinsip terkait ke dalam undang-undang federal. *Securities and Exchange Commission* (SEC) dan *Public Companies Accounting Oversight Board* (PCAOB) telah mengeluarkan panduan mengenai topik ini. *Committee on Sponsoring Organizations* (COSO) juga telah berupaya signifikan dalam penilaian risiko, menghasilkan model COSO untuk penilaian risiko perusahaan. Meskipun demikian, statistik kecurangan (seperti yang disampaikan pada Bab 2) menunjukkan bahwa jumlah keseluruhan dugaan kecurangan relatif konsisten, tetapi kerugian dari kecurangan yang terungkap terus meningkat.

Dasar dari tata kelola perusahaan yang efektif, pengendalian internal, program anti kecurangan, dan penyelidikan kecurangan adalah penilaian risiko yang menyeluruh. Penilaian risiko kecurangan yang efektif bergantung pada pemahaman tentang konsep kecurangan seperti segitiga kecurangan, *red flag*, skema kecurangan, dan sistem informasi akuntansi. Semua ini harus dipertimbangkan dalam konteks lingkungan kecurangan yang ada, termasuk entitas, kerangka waktu, dan efektivitas pengendalian internal saat ini. Meskipun istilah "penilaian risiko" mungkin terdengar seperti kegiatan periodik, manajemen risiko yang baik memerlukan proses yang berkelanjutan dan terus menerus. Bab ini membahas konsep dan alat untuk penilaian risiko guna mendukung proses tersebut. Meskipun disajikan terutama dari perspektif internal entitas, konten ini juga relevan untuk penyelidikan kecurangan eksternal dan pemangku kepentingan eksternal lainnya.

B. LITERATUR TEKNIS DAN PENILAIAN RISIKO

Gagasan penilaian risiko telah menjadi bagian penting dari literatur teknis audit, dengan audit yang kini disarankan atau diwajibkan untuk memasukkan penilaian risiko. Standar audit dalam beberapa tahun terakhir mencerminkan peningkatan fokus pada cakupan risiko. Untuk perusahaan publik, Standar *Auditing* PCAOB No. 5 (AS5), yang diadopsi pada tahun 2007, dibangun berdasarkan standar sebelumnya, PCAOB No. 2 (AS2), dengan memperluas peran penilaian risiko. AS2 mengatasi penilaian risiko dari perspektif

BAB 6
PENCEGAHAN KECURANGAN

A. PENGANTAR

Saat mengembangkan sistem pengendalian kecurangan, sangat sulit untuk mengetahui apa yang harus dilindungi dan bagaimana melindunginya jika seseorang tidak melakukan penilaian risiko terlebih dahulu untuk melihat di mana letak risiko pada suatu entitas (kecuali kecurangan yang telah terjadi). Itu termasuk aset dengan risiko paling tinggi, skema kecurangan paling mungkin terjadi adalah *red flag*, dan risiko residual. Mengingat kontrol apa yang sudah ada untuk mengurangi risiko yang ada. Pencegahan kecurangan dan penilaian risiko (Bab 5) keduanya layak untuk didiskusikan secara menyeluruh, jadi mereka berpisah dalam buku ini.

Tujuan dari setiap program anti kecurangan ini adalah untuk mencegah terjadinya kecurangan, tidak hanya untuk mendeteksinya. Aksioma lama "Satu ons pencegahan bernilai satu pon penyembuhan" adalah pernyataan yang meragukan dalam konteks kecurangan. Bagian dari *Sarbanes-Oxley* (SOX) *Act of* 2002 mengandung prinsip-prinsip hukum yang bertujuan mencegah kecurangan. Meskipun mendeteksi kecurangan itu penting, lebih baik jika kecurangan dapat dikurangi atau dicegah sebanyak mungkin. Deteksi dan pencegahan kecurangan saling berkaitan, dan keduanya bersama-sama menciptakan sistem kontrol anti kecurangan. Bab ini menjelaskan komponen-komponen dari sistem kontrol anti kecurangan yang efektif.

B. PENCEGAHAN LINGKUNGAN

Kunci sukses pencegahan kecurangan adalah dengan melihat budaya entitas dan mencoba untuk mengubahnya, jika diperlukan. Beberapa tindakan dan sikap bisa membantu mencapai tujuan ini. Unsur-unsur pencegahan yang akan dibahas selanjutnya biasanya diterapkan pada organisasi secara umum, dan tidak selalu terkait dengan jenis kecurangan tertentu.

- **Struktur Tata Kelola Perusahaan**

Sebelum adanya SOX, penelitian menunjukkan bahwa tata kelola perusahaan yang lemah sering dikaitkan dengan kecurangan keuangan besar. Misalnya, The COSO Landmark Study (1998) mempelajari 200 dari 300 kasus kecurangan yang ditangani oleh *Securities and Exchange Commission* (SEC) dari tahun 1987 hingga 1997. Penelitian ini menemukan bahwa perusahaan

BAB 7
DETEKSI KECURANGAN

A. PENDAHULUAN

Bab 1 hingga Bab 4 dalam buku ini menjelaskan secara terperinci tentang strategi efektif untuk mendeteksi kecurangan. Bab 1 memberikan gambaran umum tentang penyelidikan kecurangan, Bab 2 mengulas teknik deteksi dini, Bab 3 membahas kemungkinan skema kecurangan, dan Bab 4 memberikan penjelasan mendalam tentang deteksi kecurangan, termasuk pengetahuan tentang empat elemen penting yakni latar belakang kecurangan, prinsip-prinsip kecurangan, skema, dan tanda-tanda peringatan atau dampak kecurangan.

Untuk mendeteksi kecurangan, pendekatan awal adalah mengidentifikasi skema kecurangan dan penyebabnya yang dapat membuatnya bertahan lama. Penyidik perlu memahami konsep seperti pohon kecurangan, segitiga kecurangan, kontrol kecurangan, dan dampaknya untuk menguji atau menolak teori yang ada. Bab ini juga mencakup pembahasan tentang aksioma dan metode deteksi kecurangan, baik yang umum maupun spesifik.

B. AKSIOMA DALAM DETEKSI KECURANGAN

Ketika merancang program atau kegiatan untuk mencegah kecurangan, penting untuk diingat beberapa prinsip dasar (aksioma) yang membantu dalam deteksi kecurangan. Kunci utama untuk mendeteksi kecurangan adalah kontrol, di mana kontrol berkaitan erat dengan pencegahan kecurangan. Tanpa adanya kontrol dalam sebuah perusahaan atau instansi, kecurangan lebih mudah terjadi. Oleh karena itu, penerapan kontrol, meskipun sederhana, sangat diperlukan. Kecurangan lebih sering terdeteksi melalui tindakan reaktif daripada tindakan proaktif, yang menunjukkan adanya peluang untuk perbaikan. Dalam konteks audit eksternal, dikenal istilah *overreliance* untuk mendeteksi kecurangan, yang dijelaskan di Bab 17 tentang perbedaan antara audit kecurangan dan audit keuangan. Selain itu, kecurangan dapat diidentifikasi melalui intuisi, kecurigaan dari penyidik, manajer, auditor, atau melalui anomali dalam catatan akuntansi. Bab ini berfokus pada kemampuan mendeteksi kecurangan secara dini.

BAB 8
RESPON KECURANGAN

A. PENGANTAR

Terdapat tiga fase dasar dari pelaksanaan program anti kecurangan, yakni fase pencegahan, fase pendeteksian, dan fase tanggapan atau respons. Ketiga fase dasar ini mirip dengan model anti kecurangan lain yang bernama PDC (*preventive-detective-corrective*) yang digunakan untuk tindakan keamanan seperti *Information Security* (InfoSec) dan rancangan kontrol dalam bidang akuntansi dan *auditing*. Dalam fase pencegahan, menyediakan *leverage* tertinggi atau *return* dilakukan untuk dapat mencegah terjadinya kecurangan. Adapun tahap respons nantinya akan dilaksanakan jika dideteksi telah terjadi tindakan kecurangan pada entitas. Hal ini dilakukan semata-mata karena keinginan entitas untuk dapat mengetahui segala kecurangan yang terjadi di dalamnya. Nantinya, manajemen harus memikirkan bagaimana respons atau tanggapan yang akan dikeluarkan sebelum kecurangan tersebut benar-benar terjadi. Secara urutan, fase ini kemungkinan berada pada tahap pertama atau kedua (fase penilaian risiko kecurangan juga berkemungkinan menjadi tahap pertama; fase ini dapat dilihat pada Bab 5) yang akan dilakukan dalam perencanaan dan pengembangan kebijakan dan prosedur untuk pelaksanaan program anti kecurangan.

B. KEBIJAKAN KECURANGAN

Kemungkinan besar, langkah terbaik yang dapat dilakukan untuk mengembangkan respons kecurangan yang efektif adalah dengan mengembangkan kebijakan kecurangan yang tepat. Ada beberapa masalah yang perlu dipertimbangkan terlebih dahulu saat menyusun kebijakan kecurangan. Pertama, pentingnya mendefinisikan kecurangan secara tepat. Sebagaimana yang tercantum dalam penjelasan Bab 2, terdapat berbagai macam definisi mengenai tindakan kecurangan. Jika definisi kecurangan tidak ditentukan sebelumnya, maka karyawan mungkin akan merasa bingung, salah paham, atau tidak setuju tentang tindakan kecurangan yang dimaksud oleh atasannya. Sebagai tambahan, dalam proses pengadilan, suatu definisi akan mengikuti interpretasi dari hakim atau juri, yang mana hal ini mungkin tidak akan sama dengan definisi yang dipikirkan oleh korban. Misalnya, jika seorang karyawan ''meminjam'' kamera digital milik atasannya untuk mengambil gambar pribadinya, menggunakan komputer atasan untuk membuat akun di ebay.com dan mengelola akun tersebut untuk menjual barangnya, serta

BAB 9
KEJAHATAN KOMPUTER

A. PENGANTAR

Teknologi memainkan berbagai peran dalam lingkungan penipuan. Sistem dan data dapat digunakan untuk mencegah, mendeteksi, dan menyelidiki penipuan. Ketika teknologi digunakan untuk melakukan penipuan, mekanisme yang digunakan biasanya adalah komputer (didefinisikan secara luas di sini sebagai perangkat yang melakukan perhitungan dan menyimpan data). Teknologi, terutama komputer dan *server*, bahkan bisa menjadi target dari pelaku kejahatan. Seiring dengan semakin terintegrasinya teknologi ke dalam masyarakat, teknologi juga semakin terintegrasi ke dalam kejahatan termasuk penipuan.

Sebelum ada komputer, tidak ada kejahatan komputer, tetapi ada kejahatan di bidang lain baik yang dilakukan oleh pelaku kerah putih maupun kerah biru. Juga ada kejahatan terhadap orang dan kejahatan terhadap properti. Komputer tidak memperkenalkan era baru dari kejahatan, tetapi menyediakan alat baru yang sangat kuat untuk melakukan kejahatan. Komputer telah membuat beberapa jenis kejahatan lebih mudah dilakukan, seperti pencurian identitas dan pencurian data skala besar.

Dengan kemajuan teknologi, para penjahat juga mengembangkan keterampilan mereka untuk mengeksploitasi kerentanan baru. Seiring dengan perkembangan teknologi, begitu pula dengan kejahatan terkait teknologi. Dalam beberapa dekade terakhir, kejahatan komputer telah menjadi isu penting di seluruh dunia. Peningkatan penggunaan internet dan teknologi jaringan telah membuka banyak peluang bagi penjahat untuk melakukan kejahatan dengan cara yang sebelumnya tidak mungkin

B. SEJARAH DAN EVOLUSI KEJAHATAN KOMPUTER

Komputer elektronik pertama kali diperkenalkan untuk penggunaan komersial di Amerika Serikat pada tahun 1954, ketika *General Electric* (GE) menjadi bisnis AS pertama yang menggunakan komputer. Sebelum tahun tersebut, beberapa komputer yang ada digunakan untuk tujuan pemerintahan seperti dimanfaatkan untuk tabulasi sensus nasional, untuk aplikasi militer, dan untuk penelitian ilmiah. Sejarah kejahatan komputer dimulai pada pertengahan 1950-an.

DAFTAR PUSTAKA

Singleton Tommie W. And Aaron J., 2010, *Fraud Auditing and Forensic Accounting, Fourth Edition*, john Willey and Sons. Inc

AKUNTANSI FORENSIK

Prof. Dr. Edy Sujana, S.E., M.Si., Ak., CA., CFrA. kelahiran 27 Juli 1973. Beliau adalah alumni S1, Akuntansi Universitas Udayana, dan menempuh S2 dan S3 pada Program Studi Ilmu Akuntansi pada Universitas Gadjah Mada dan Universitas Airlangga. Saat ini Prof. Edy merupakan Guru Besar dan Dosen tetap pada Program Studi Akuntansi S1 dan S2 pada Universitas Pendidikan Ganesha.

Beliau telah mengampu mata kuliah *Auditing* sejak tahun 1999 dan mengampu mata kuliah Akuntansi Forensik sejak mata kuliah ini mulai diperkenalkan di Program S1 Akuntansi sekitar 10 tahun yang lalu. Selain sebagai Dosen Prof. Edy juga aktif sebagai Akuntan berpraktek dan aktif sebagai konsultan diberbagai organisasi. Selain itu beliau juga aktif dalam keanggotaan Organisasi Akuntan Forensik di Indonesia.

ISBN 978-623-500-277-4

Penerbit widina
www.penerbitwidina.com