Prosiding National Seminar on Accounting, Finance, and Economics (NSAFE), 2022, Vol. 2 No. 6, Hal 53-62.

No. ISSN 2797-0760

Peran Auditor Teknologi Informasi Dalam Mengurangi Kejahatan Komputer
(SEBUAH STUDI PUSTAKA)

Brian Firmansyah Putras[1*], Abdul Aziz Wahyu Alamsyah[2],Tomy Rizky Izzalqurny[3]
[1,2]Universitas Jember
[3]Universitas Negeri Malang

*brianfirmansyah123@gmail.com

Abstrak
Teknologi Data kini telah menjadi kebutuhan mendasar bagi hubungan industri untuk mengurus pengiriman dan pekerjaan dengan persiapan yang diadakan di dalam asosiasi. Inovasi informasi berbasis PC secara keseluruhan mempengaruhi masyarakat saat ini, terutama untuk afiliasi industri. Saat ini, asosiasi modern dihadapkan pada iklim yang berubah dengan cepat dan kejam. Dengan demikian, tempat inovasi informasi penting bagi asosiasi modern untuk membantu pengembangan bisnis dan arah mandiri. Penggunaan inovasi informasi dapat menghilangkan kontrol internal dengan mengembangkan lebih lanjut teknik-teknik baru yang dicoba oleh komputer serta kontrol manual yang mengandalkan kesalahan manusia. Inovasi informasi juga dapat menghadirkan bahaya baru. Penguji harus berhati-hati agar tidak terlalu bergantung pada data yang dihasilkan oleh PC. Peninjau harus mendominasi dan menguji kontrol berbasis PC sebelum menyimpulkan bahwa informasi yang dihasilkan PC dapat diandalkan.
Kata Kunci: Teknologi Informasi, Pengendalian, Pc

Abstract
Data Technology has now turned into a fundamental requirement for industry relationship to take care of convey and work with the preparation held inside the association. PC based information innovation altogether affects the present society, particularly for industry affiliations. Today, modern associations are confronted with a quickly changing and cutthroat climate. Accordingly, the place of information innovation is significant for modern associations to help business development and independent direction. Use of information innovation can chip away at the inner control by further developing the new techniques that are attempted by the pc as well as manual controls which rely upon human mistake. Information innovation can likewise present new dangers. Examiners should be mindful so as not to depend a lot on data produced by the PC. Reviewers should dominate and test PC-based controls prior to concluding that PC-produced information is dependable
***Keywords**: Information Technology, Control, PC*

PENDAHULUAN

Berbicara tentang sistem Informasi, hampir seluruh aspek manusia telah dikombinasi dengan kemajuan teknologi. Kegiatan sehari-hari kita bekerja tidak luput dari adanya perkembangan teknologi informasi. Adanya kemajuan teknologi informasi ini diharapkan mampu meringankan segala aktivitas manusia. Namun apakah benar begitu? Di negara maju perkembangan teknologi informasi sangat berjalan sangat cepat, dikarenakan sumber daya manusianya yang memang mendukung dalam hal ini. Jika kita melihat kondisi Indonesia di tengah perkembangan teknologi informasi, penduduk Indonesia belum 100% dapat mengikuti arus kemajuan jaman yang sangat cepat. Imbasnya banyak tenaga kerja yang harusnya menjadi

milik penduduk Indonesia menjadi milik warga negara asing. Sumber daya manusia di Negeri kita ini harus memang sebaiknya ditempa sedemikian sehingga memiliki kemampuan yang dapat bersaing dengan negara lain.

Audit adalah profesi yang menganalisis suatu data/bukti keuangan yang nanti akan disesuaikan dengan standar yang berlaku umum. Ketika auditor melaksanakan auditnya tidak selalu berpegang dengan kemampuan konseptual serta teori-teori yang berlaku umum, Namun juga skill dalam menerapkan teknik-tekniknya. Di masa perkembangan teknologi sekarang ini, auditor dibantu dengan adanya komputer, komputer memiliki peran yang sangat kompleks ketika melakukan audit. Hampir seluruh data transaksi akuntansi hingga prosedur melakukan audit telah menggunakan komputer. Tentu saja, sebagai auditor internal maupun eksternal harus memiliki skill dalam menggunakan piranti komputer sebagai bahan dalam prosedur audit.

Meningkatnya penggunaan teknologi informasi mengharuskan auditor untuk memasukkan bukti audit elektronik ke dalam audit mereka. Banyak data akuntansi seperti jurnal umum, buku besar, pengiriman uang, faktur dan data keuangan lainnya saat ini hanya tersedia dalam format elektronik (soft copy). Persyaratan audit mengharuskan auditor dapat menggunakan teknik yang lebih canggih serta efektif dalam pengambilan keputusan, penyimpanan informasi, dan berbagai fungsi audit lainnya. Auditor juga perlu mempelajari melakuakn evaluasi dan mengevaluasi berbagai teknik yang digunakan oleh auditee dan mengidentifikasi peluang untuk mengadopsi teknik yang lebih canggih agar dapat melakukan fungsi audit secara lebih efisien dan efektif. Teknologi informasi dapat menjadi alat yang sangat berharga untuk melakukan kegiatan audit secara lebih efektif dan efisien.

Kemajuan TI tidak hanya berdampak positif terhadap kemajuan dalam banyak hal, tetapi juga memiliki efek samping negatif dari segi risiko dan potensi gangguan. Hal ini dipengaruhi oleh faktor-faktor yang menentukan keberhasilan dan keberlanjutan suatu perusahaan. Oleh karena itu, untuk mengelola sistem informasi berbasis komputer, diperlukan faktor keamanan dan pengendalian internal untuk mengantisipasi, mendeteksi, dan mengevaluasi berbagai kemungkinan kejahatan, kesalahan, atau penipuan komputer.

KAJIAN PUSTAKA

Pengauditan(Audit)

Sukrisno Agoes (2004:4), Pemeriksaan yang sebelumnya dilakukan oleh Pemeriksa beserta bukti dan data , dilakukan secara independen, sistematis dan kritis, dengan tujuan agar Pemeriksa dapat menyatakan pendapatnya tentang kebenarannya. laporan keuangan yang disiapkan.

Sistem Informasi Akuntansi

Mulyadi (2015) mengemukakan bahwa sistem informasi akuntansi yang dibuat oleh manajemen untuk kebutuhan, harus ketika sistem informasi dibuat harus mencakup tujuan lain.

Audit Forensik

Tinjauan pengadilan terkemuka membutuhkan strategi pembukuan tinjauan dan tinjauan kemampuan yang sah. Untuk situasi ini, pengujian hukum mencakup berbagai latihan berwawasan yang sering dilakukan untuk mendakwa pihak atas pemerasan, penyelewengan, atau

kesalahan moneter lainnya. Selama interaksi awal, inspektur akan diberi konseling sebagai master kasus. Selain kemajuan di atas, tes kriminologi ini juga dapat diingat untuk keadaan seperti perdebatan kepailitan, pemerasan bisnis dan pemisahan. Tes terukur dapat mengungkap atau menegaskan operasi kriminal yang berbeda. Dengan demikian, ulasan ilmiah lebih penting daripada ulasan standar.

Kejahatan Komputer

Pelanggaran digital (cybercrime) adalah pelanggaran yang dilakukan melalui inovasi web dengan mengejar data terbuka dan rahasia yang bersifat pribadi atau rahasia di internet. Ini menyerupai sambaran petir yang melenyapkan kekuatan informasi yang seimbang dan realitas data.

Model kesalahan di atas dapat berupa kesalahan terputus, kesalahan semi online, dan kesalahan digital. Masing-masing kegiatan ini memiliki atributnya masing-masing. Pelanggaran dapat dilakukan di mana saja, baik di dunia nyata maupun di internet. Ini karena periode tumbuhnya pintu terbuka untuk kesalahan, dan harus cenderung secara agregat melalui partisipasi mitra kita. erat kaitannya dengan kemajuan masyarakat.

Kejahatan PC adalah demonstrasi melawan hukum yang merugikan satu pihak dengan melibatkan PC sebagai metode/alat atau dengan mendapatkan PC. Pelanggaran PC dicirikan sebagai demonstrasi melanggar hukum yang dilakukan dengan memanfaatkan inovasi PC canggih. Perbuatan salah dapat dilakukan di mana saja, baik di ruang nyata maupun di internet. Hal ini karena perkembangan zaman globalisasi di arena publik, akibatnya berbagai komponen masyarakat harus dijunjung tinggi untuk bekerja sama melakukan apa pun untuk mencegah dan menghancurkan perbuatan salah.

Kejahatan PC adalah perbuatan salah yang dilakukan dengan melibatkan media sebagai objek PC. Jadi, pelanggaran PC dicirikan sebagai demonstrasi melanggar hukum yang dilakukan dengan memanfaatkan inovasi PC yang lebih maju.

UU Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008

Pasal 30 Undang-Undang Nomor 11 Tahun 2008 mengatur tentang perbuatan yang diingkari, yaitu akses khusus yang melanggar hukum. Breaking dan Hacking penting untuk akses yang melanggar hukum. Pasal 30 UU ITE membaca dengan teliti:

1. Setiap individu dengan sengaja dan tanpa hak istimewa atau ilegal mendapatkan PC orang lain dan kerangka kerja elektronik tambahan dalam kapasitas apa pun.
2. Setiap individu dengan sengaja dan tanpa hak istimewa atau ilegal mendapatkan PC atau kerangka kerja elektronik yang berpotensi dalam kapasitas apa pun yang ditentukan untuk mendapatkan data elektronik serta catatan elektronik.
3. Setiap orang yang dengan sengaja dan tanpa hak istimewa atau melawan hukum mengakses PC dan sistem elektronik dalam kapasitas apa pun mengabaikan, melewati, melampaui, atau merusak kerangka keamanan.

Pengaturan curang Pasal 30 UU ITE diarahkan dalam Pasal 46 UU ITE yang membaca:

1. Setiap orang yang memenuhi komponen sebagaimana dimaksud dalam Pasal 30 ayat

2. dipidana dengan pidana kurungan paling lama 6 (enam) tahun atau denda paling banyak Rp. 600.000.000,00 (600.000.000 rupiah).
3. Setiap orang yang memenuhi komponen sebagaimana dimaksud dalam Pasal 30 ayat
4. dipidana dengan pidana kurungan paling lama 7 (tujuh) tahun dan denda paling banyak Rp. 700.000.000,00 (700.000.000 rupiah).
5. Setiap orang yang memenuhi komponen sebagaimana dimaksud dalam Pasal 30 ayat
6. dipidana dengan pidana kurungan paling lama 8 (delapan) tahun dan pidana denda paling banyak Rp. 800.000.000,00 (800.000.000 rupiah)..

METODE PENELITIAN

Jenis dan Sumber Data

Studi ini menggabungkan gambaran yang dihitung yang memberikan persepsi dan data pemeriksaan tentang pekerjaan pemegang buku dalam mengurangi kesalahan PC. Jenis pemeriksaan, sekali lagi, memasukkan audit penulisan yang akurat, atau yang biasanya disingkat SLR, dan mengatur teknik analisis yang sah. Sepanjang garis ini, pencipta memperhatikan, meringkas, dan menguraikan penemuan semua masalah yang berhubungan dengan titik eksplorasi tertentu (Kitchenham dan Cahrters, 2017). Teknik standarisasi pemeriksaan yang sah dengan mengumpulkan bahan pustaka.

Informasi ulasan semacam ini adalah informasi opsional. Informasi penunjang adalah bahan pustaka, meliputi arsip dinas, buku perpustakaan, pedoman hukum, karya logika, artikel, dan laporan bahan eksplorasi. Informasi opsional dapat diperoleh dari berbagai sumber, termasuk bahan-bahan penting, tambahan, dan tersier yang sah. Informasi yang diperoleh ditangani dan diselidiki untuk menanggapi pertanyaan saat ini.

Teknik Pengumpulan Data

Seperti yang ditunjukkan oleh Sula, et al. (2014), menulis studi adalah tinjauan yang menguraikan lebih baik pemeriksaan masa lalu dan diakhiri dengan studi menulis dengan konsekuensi dari penyelidikan dasar dan pengaturan yang layak terkait dengan isu-isu yang diangkat oleh spesialis. Para ahli mengumpulkan berbagai informasi terkait dengan masalah yang sedang dieksplorasi melalui buku harian, web, buku, dan berbagai perangkat yang terkait dengan tugas pengulas dalam mengurangi kesalahan PC di masa globalisasi yang sedang berlangsung.

HASIL DAN PEMBAHASAN

Permasalahan Kejahatan Komputer dalam Hukum Pidana

Di berbagai negara, langkah-langkah yang sah untuk mengurangi jumlah pelanggaran PC terus dicari. Garis besar kemajuan administratif yang diambil untuk mengelola kesalahan representasi oleh kontrol PC. Dalam kerangka anggaran Kontinental ini biasanya berusaha untuk dikalahkan dengan menggunakan pengaturan keuangan yang berhubungan dengan penipuan dan penipuan, sedangkan di negara- negara Anglo Amerika akan secara umum menghubungkan atau memasukkannya (misalnya; dalam hal toko uang) dalam pengaturan pengaturan tentang perampokan dan penyelewengan.

Pada dasarnya menghubungkan kesalahan PC dengan pelanggaran adat tidak sesederhana itu. Misalnya, untuk perampokan dan penyelewengan, penting untuk bertindak dengan mengambil milik orang lain. Masalah akan muncul ketika pelakunya mengambil toko yang terkait dengan menggunakan uang tunai distributor. Demikian pula halnya dengan demonstrasi kriminal pemerasan (misrepresentasi) yang di berbagai negara seharusnya menjadi syarat bahwa seseorang yang ditipu adalah PC. Ini sulit diterapkan jika cheatnya adalah PC. Jika dilihat secara keseluruhan, kasus-kasus yang muncul adalah; apakah informasi penyimpanan elektronik adalah laporan yang disalahpahami, meskipun faktanya hal ini umumnya memerlukan penjelasan yang dapat diperiksa dan diteliti.

Terjemahan bermasalah yang berbeda mempengaruhi tahap otoritatif yang akan diambil. Metodologi utama yang dapat diambil dengan cara tersebut dipandang sebagai metodologi dunia, yang memerlukan pedoman non-eksklusif lain dari pelanggaran PC yang memasukkan berbagai jenis tindakan, seperti; kontrol, pemusnahan, perampokan, dan penggunaan PC yang tidak disetujui (masuk ke DP-framework). Ini harus terlihat, misalnya, dalam Undang-Undang Data Swedia, 1973.

Risiko Teknologi Komputer dan Internet

Internet adalah organisasi kerangka kerja inovasi data terbesar dan dapat menghubungkan perangkat di mana-mana. Karena jangkauan organisasi web yang luas, inovasi data ini umumnya berdampak buruk pada kliennya. Jaringan web terbuka yang mengkomunikasikan informasi menggunakan standar Internet Protocol (IP). Data yang disebarluaskan di Internet dapat diperoleh melalui jaringan World Wide Web (www) sebagai teks, musik, foto, rekaman, atau konfigurasi yang berbeda. Awalnya, Internet adalah jaringan PC yang dibuat oleh Departemen Pertahanan AS pada tahun 1969 sebagai fitur dari Proyek ARPA (Defense Advanced Research Projects Agency). Sejak saat itu, ARPA memilih untuk berkonsentrasi pada cara terbaik untuk menghubungkan beberapa PC ke organisasi alami. Manfaatkan saluran telepon untuk menghubungkan beberapa PC berbasis UNIX yang jauh sehingga PC ini dapat berbicara satu sama lain. UNIX adalah kerangka kerja PC yang dimulai pada tahun 1965 dengan proyek Multics.

Usaha tersebut kemudian, pada saat itu, merencanakan keadaan organisasi, kualitasnya yang tak tergoyahkan, dan berapa banyak informasi atau data yang dapat dipindahkan mulai dari satu PC lalu ke PC berikutnya. Jaringan utama dibangun terkait empat tujuan: University of California, Los Angeles (UCLA), University of California, Santa Barbara (UCSB), University of Utah, dan Stanford Institute (SRI). Pada tahun 1972, Internet memiliki lebih dari 20 PC terkait. ARPANet adalah tulang punggung internetworking untuk individu yang terlibat dengan sekolah, penelitian, industri, pekerja untuk disewa, dan khususnya organisasi militer.

Berikut beberapa dampak buruk dari penggunaan internet:

A. Membuat klien terlepas dari kolaborasi ramah langsung.
B. Meningkatkan penyebaran infeksi PC.
C. Tidak ada yang menjamin keabsahan atau keakuratan data.
D. Memudahkan seseorang untuk menduplikasi yang dibuat oleh orang lain.
E. Membuka pintu lebar-lebar bagi individu yang tidak bertanggung jawab melakukan pelanggaran.

F. Membahayakan keamanan data yang diklaim oleh semua orang, misalnya pengelola uang dan otoritas publik.

Keamanan dan Pengendalian Sistem Informasi Berbasis Komputer

Keamanan kerangka mencirikan berbagai cara untuk mencegah orang yang tidak disetujui, termasuk penyusup, agar tidak menyimpan data. Anda harus memenuhi variabel yang harus dipikirkan saat membuat kerangka data pembukuan. Pedoman kecepatan adalah menyediakan data yang benar-benar Anda inginkan dengan kualitas yang tepat, cepat dan tepat waktu.

- Aturan keamanan yang membantu menjaga sumber daya Anda tetap aman.
- Standar biaya minimal, khususnya biaya pelaksanaan kerangka data pembukuan harus dikurangi.
- Kekhawatiran yang lebih menonjol dalam menjalankan kerangka kerja keamanan kerangka data adalah untuk membatasi celah bagi pelaku untuk memperlambat kerangka kerja data atau proyek, baik melalui PC, lingkungan atau organisasi di seluruh dunia.

Oleh karena itu, harus dijamin bahwa kerangka kerja berjalan dengan benar dan semuanya tampak hebat dengan aplikasi.

- Pemicu Kejahatan Komputer
- Beberapa hal yang dapat memicu terjadinya kejahatan komputer adalah:
- Penggunaan komputer dan internet yang semakin marak
- Penyalahgunaan software, yaitu dengan mencari celah yang ada kemudian digunakan untuk melakukan scanning terhadap sistem lain.
- Banyak perangkat lunak yang dapat mendukung pelaku kejahatan dalam melakukan tindakannya.
- Keterbatasan SDM sehingga mudah untuk terserang tindak kejatan sistem informasi
- Banyaknya kegiatan perusahaan sekarang yag terhubung ke LAN
- Maraknya bug sekarang ini.

Cara paling basic untuk memperkuat keamanan komputer anda dengan cara membatasi akses fisik komputer, mengkonfigurasi mekanisme perangkat lunak dan sistem operasi, dan menetapkan strategi pemrograman untuk membuat program komputer lebih andal. Hal ini harus dilakukan guna menangkal pelaku yang tidak berwenang mengakses komputer Anda. Keamanan komputer sangat penting karena berkaitan dengan privasi, integritas, otentikasi, kerahasiaan, dan ketersediaan.

Keamanan Internet

Dengan kekuatan internet yang dapat menghbungkan dunia luar tanpa melibatkan material fisik mengakibatkan keamaan fisik tidak akan berguna jika diterapkan dalam prosedur keamaan sistem informasi. Misalnya, Jika perusahaan menempatkan komputer di tempat terkunci dan terpencil yang tidak semua orang tau, namun belum tentu komputer tersebut aman dari jangkauan internet. Penyebab dari tindak kejahatan sistem informasi dapat terjadi akibat dari kelemahan sumber, antara lain sebagai berikut:

1. Sistem operasional atau konfigurasinya.

2. Web server atau konfigurasinya.
3. Jaringan server dan konfigurasinya.
4. Program server dan konfigurasinya.
5. Lemahnya prosedur keamaan sistem informasi. Keamanan Dalam Sistem Informasi Akuntansi

George H. Bodnar dan William S. Hopwood (2001) menyatakan terdapat enam metode yang dilakukan oleh pelaku penipuan dan kejatahan sistem informasi, antara lain metode sebagai berikut:

1. Memanipulasi
2. Mengubah program
3. Manipulasi Arsip secara langsung
4. Mencuri data
5. Perongrongan/Sabotase sistem informasi
6. Tindak penyalahgunaan sistem informasi oleh pelaku.

Sistem Keamanan Informasi

Sistem keamanan informasi merupakan suatu subsistem dalam suatu organisasi yang bertugas mengendalikan risiko terkait dengan sistem informasi berbasis-komputer.

- Efektifitas
- Efisiensi
- Kerahaasiaan
- Integritas
- Keberadaan (availability)
- Kepatuhan (compliance)
- Keandalan (reliability)

Foresik Komputer

Pengertian Komputer Forensik Menurut Para Ahli Judd Robin

Kriminologi PC adalah ide dasar pemeriksaan PC dan metode ilmiahnya dalam memutuskan berbagai konfirmasi sah yang mungkin.

Bangsawan

Ilmu hukum PC berperan penting dalam memulihkan, mengikuti, memulihkan, dan memperkenalkan informasi yang telah ditangani secara elektronik dan disimpan di media PC. (Ruby Alamsyah) Kriminologi komputer atau komputerisasi kriminologi seharusnya menjadi ilmu yang meneliti pembuktian dengan cermat untuk dipikirkan di pengadilan. Bukti lanjutan termasuk, namun tidak terbatas pada, workstation, sel, bantalan awal, dan perangkat khusus lainnya yang memiliki ruang ekstra dan dapat diperiksa.

Alasan untuk Komputer Forensik

Alasan untuk investigasi TKP PC adalah untuk melindungi dan memecah bukti lanjutan dan untuk mendapatkan realitas objektif dari kejadian kerangka data atau gangguan keamanan. Realitas ini digunakan sebagai bukti dalam pendahuluan. Misalnya, melalui kriminologi Internet, Anda dapat mengetahui siapa yang mengirim email, kapan dan di mana itu. Dalam model lain,

Anda dapat melihat siapa tamu situs Anda, alamat IP mereka, PC dan area yang Anda gunakan, dan data tentang pergerakan yang dilakukan di situs Anda..

Tahapan pada Komputer Forensik

Terdapat empat fase dalam komputer forensik, antara lain yaitu:

1. Pengumpulan data, tujuannya mengidentifikasi berbagai sumber daya yang dianggap mendesak, dan mengidentifikasi cara mengumpulkan seluruh data dengan benar.
2. Tes, uji, berbaris berbagai informasi tentang berbagai fungsi sistem operasi dan aplikasi yang dapat mengurutkan berbagai informasi tentang semua data yang dikumpulkan yang dikumpulkan untuk menghindari proses atau menghapus data yang diganti. B. Enkripsi, Kompresi, Mekanisme Kontrol Akses, File Periodik, Tes Penugasan Data, Ekstraksi File, dll.
3. Analisis, dapat terjadi dengan cara yang berbeda. Tantangan analisis ini berisi banyak kegiatan, misalnya. B. Secara tidak langsung, identifikasi pengguna (pengguna) mengingat bagaimana lokasi, institusi, perangkat, dan semua komponen harus terhubung untuk mendapatkan kesimpulan akhir.
4. Dokumen dan laporan, dan hasil lain, ada beberapa faktor seperti ini.

Deskripsi lain (penjelasan alternatif) - Analis pada dasarnya harus menggunakan pendekatan dalam bentuk prosedur untuk menyetujui atau menolak kasus atau deskripsi kasus yang diajukan. Pertimbangan Audiens-Ini untuk memberikan Audiens dengan data atau informasi yang sangat berguna dan diperlukan.

Jika beberapa aturan terlibat, Anda memerlukan laporan spesifik dari informasi data yang Anda kumpulkan. Selain itu, sangat penting untuk memiliki salinan semua fakta yang diterima. Ini karena Anda dapat membuat refleksi yang sangat bijaksana. Informasi Praktis – Ini adalah proses dokumentasi dan pelaporan yang melibatkan identifikasi informasi praktis yang dikumpulkan dari berbagai data historis. Dengan bantuan data ini Anda bisa mendapatkan informasi terkini dan menyebutnya.

Fungsi Komputer Forensik

A. Membantu memulihkan, menganalisis, & menyajikan materi/badan berbasis digital atau elektro sedemikian rupa sebagai akibatnya bisa dipakai menjadi indera bukti yg absah pada pengadilan; &
B. Untuk mendukung proses identifikasi barang bukti pada ketika yg nisbi cepat, sebagai akibatnya bisa diperhitungkan asumsi imbas potensial yg disebabkan sang konduite kriminal yg dilakukan sang pelaku kejahatan terhadap korbannya, dan menyampaikan alasan & motivasi tindakan tadi sembari mencari bagi pihak-pihak terkait yg terlibat pribadi juga nir pribadi. nir pribadi menggunakan perbuatan nir menyenangkan tadi.
C. Kegiatan forensik personal komputer umumnya dilakukan pada 2 konteks utama. Yang pertama merupakan konteks yg berkaitan menggunakan pengumpulan & penyimpanan data yg berisi seluruh catatan rinci aktivitas rutin yg dilakukan sang organisasi atau perusahaan eksklusif yg melibatkan teknologi kabar & komunikasi.

Dan yg ke 2 merupakan pendataan yg secara spesifik ditujukan pada konteks kejahatan berbasis teknologi.

Peran Auditor Forensik

Tugas penguji hukum dalam penghindaran pemerasan, lokasi, dan pemeriksaan tidak sama dengan tugas penilai bebas sebagai pengulas dalam ringkasan anggaran. Pembukuan yang ditegaskan berpusat di sekitar menjamin bahwa pembukuan organisasi (uang tunai) di mana penilaiannya signifikan adalah adil. Mengingat hal ini, kewajiban evaluator adalah untuk merencanakan dan melaksanakan strategi peninjauan di tempat yang tepat dan mengenali kesalahan kutipan material dalam ringkasan fiskal yang diperkenalkan tanpa membedakan alasan kesalahan atau perbedaan tersebut.

Pembukuan pengadilan memiliki wilayah kebutuhan yang berbeda bergantung pada pekerjaan mereka. Jelas kita sangat menginginkan instrumen yang berbeda, sudut pandang yang berbeda, perspektif yang berbeda. Pada tingkat yang lebih mendalam, pertimbangan spesialis kriminologi berasal dari bukti dan pernyataan bahwa seseorang, apa, kapan, di mana, bagaimana, dan mengapa sesuatu dianggap atau diketahui tidak pantas, adalah dalam perbaikan data nyata yang diperinci.

Istilah pemeriksaan dan materialitas biasanya tidak digunakan untuk mencirikan sejauh mana metode pembukuan legal. Semua hal dianggap sama, semua bukti yang relevan dicari dan diteliti. Mengingat akibat-akibat dari pemeriksaan tersebut, pemeriksa ilmiah akan memimpin pemeriksaan dan melakukan apa saja untuk memulihkan kemalangan atau kerugian bagi perkumpulan. Kemudian, pada saat itu, menyarankan dan melakukan kegiatan perbaikan. Ini sering mencakup perubahan siklus dan pengaturan, serta bergerak melawan staf pembukuan. Selanjutnya, pemeriksa hukum menghindari potensi risiko untuk mengatasi kemungkinan terulangnya masalah tersebut. Penemuan-penemuan dan usulan-usulan para ahli ilmiah dapat digunakan sebagai alasan untuk dinyatakan dalam prosedur yang sah atau pidana terhadap pelaku kesalahan penyajian.

SIMPULAN

Pada sistem informasi berbasis teknologi dan dan jaringan internet, factor yang paling penting ialah keamanan dan tata pengendalian yang harus dapat dikelola secara efektif. Karena semakin beragamnya kejahatan yang ada di dunia system informasi berbasis teknologi dan internet. Konsep yang dilakukan untuk mengelola keamanan dan pengendalian sistem informasi berbasis teknologi dan keamanan: 1. Melakukan tindak preventif (mencegah atau mengantisipasi) terjadinya penyimpangan, kejahatan, atau tindak kejahatan lainnya yang kemungkinan terjadi. 2.Mendeteksi adanya indikasi kejahatan teknologi. 3.Melakukan evaluasi terhadap sistem informasi.

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaann teknologi informasi yang berbasis computer dan internet seperti pencemaran nama baik yang banyak terjadi di dunia sosial media. Kejahatan yang dilakukan dengan masuk ke dalam suatu sistem jaringan komputer secara illegal tanpa sepengetahuan pemilik sistem atau kejahatan dengan menggunakan serta memalsukan informasi ke web terhadap sesuatu yang salah dan tidak pantas. Ada juga bentuk kejahatan dalam pusaran teknologi informasi dengan menyebarkan berita-berita

bohong(hoax) yang sumbernya masih belum jelas namun telah di serukan dalam sosial media dengan maksud menjatuhkan suatu oknum atau membuat suatu oknum menjadi jelek di kalangan masyarakat.

Konsentrasi UU ITE 2008, penyelenggaraan forensic computer, serta keterlibatan auditor IT adalah langkah nyata terhadap upaya-upaya dalam mengurangi angka kejahatan komputer. Di luar itu, pastinya harus memerlukan dukungan dari berbagai elemen dalam menyikapi segala bentuk kejatahan maupun kecurangan komputer yang dilakukan oknum tertentu. Pemberian sanksi yang tergas dan tertulis, sikap indepedensi penegak hukum adalah faktor yang paling penting dalam menyelesaikan kasus yang terjadi di bidang sistem informasi berbasis informasi dan teknologi..

DAFTAR PUSTAKA

Anwar, Achmad Syaiful Hidayat. "PERAN AUDITOR TEKNOLOGI INFORMASI DALAM MENGURANGI KEJAHATAN KOMPUTER," no. 11 (t.t.): 16.

Dua, Jurnal Surya Kencana. "Bima Guntara Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan " 5 (2018): 17.

Hasibuan, Muhammad Siddik. "KEYLOGGER PADA ASPEK KEAMANAN KOMPUTER" 03 (2016): 8.

Prasetya, Wahdah, dan Puti Priyana. "Pertimbangan Hakim Atas Penghadiran Bukti Digital Forensik dalam Perkara Kejahatan Fraud." Wajah Hukum 5, no. 2 (15 Oktober 2021): 448. https://doi.org/10.33087/wjh.v5i2.472.

Prima Putra, Ikhsan Yusda. "PROSPEK PENGATURAN KEJAHATAN KOMPUTER DI MASA MENDATANG." JURNAL TEKNOIF 6, no. 1 (30 April 2018): 24–31.

https://doi.org/10.21063/JTIF 2018.V6.1.24-31.

Rahmansyah, Andi Ilham, dan Dedi Darwis. "SISTEM INFORMASI AKUNTANSI PENGENDALIAN INTERNAL TERHADAP PENJUALAN (STUDI KASUS : CV.

ANUGRAH PS)." Jurnal Teknologi dan Sistem Informasi 1, no. 2 (t.t.): 9.

Suryani, Indrika Dwi Rahma, Elia Kurniawati, Gracia Angelina Nawang Wulan, dan Hikmah Cahya Dinniah. "KONSEPTUALISASI PERAN TEKNOLOGI INFORMASI DALAM PRAKTIK AUDIT UNTUK MEMBANTU PENGUNGKAPAN FRAUD DI

INDONESIA." El Muhasaba Jurnal Akuntansi 12, no. 2 (22 Juli 2021): 138–56. https://doi.org/10.18860/em.v12i2.12070.

Tumalun, Brisilia, dan Dr Wempie Jh Kumendong. "UPAYA PENANGGULANGAN KEJAHATAN KOMPUTER DALAM SISTEM ELEKTRONIK MENURUT PASAL 30 UNDANG-UNDANG NOMOR 11 TAHUN 2008," no. 2 (t.t.): 8.