MENGENAL JENIS JENIS AUDIT SISTEM INFORMASI BESERTA RESIKONYA

Eka Mei Ristianti

165100091

Fakultas Komputer

ekameiristianti.student@umitra.ac.id

Abstract

Audit sistem informasi atau Information System Audit disebut juga EDP Audit (Electronic Data Processing Audit) / Computer audit merupakan suatu proses dikumpulkannya data dan dievaluasinya bukti untuk menetapkan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian, internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer.

Jenis – Jenis Audit Sistem Informasi dibagi atas 3 jenis yaitu Jenis audit berdasarkan luas pemeriksaan yaitu General audit (pemeriksaan umum) dan Special audit (pemeriksaan khusus). Tiga Jenis Manajemen Audit berdasar keragaman departemen yaitu Internal Audit, External audit, dan Extrinsic Audit Management. Pembagian jenis audit yang sejenis yaitu Audit Internal dan Audit eksternal. Audit berdasarkan bidang yaitu Audit laporan keuangan, Audit kepatuhan/ketaatan, Audit operasional, dan Audit Forensik

Adapun risiko Audit atau Audit Risk (AR) adalah kemungkinan risiko salahsaji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat.

Kata Kunci : Pengertian, Jenis-jenis, dan Risiko Audit Sistem Informasi .

A. PENDAHULUAN

Audit sistem informasi atau Information System Audit disebut juga EDP Audit (Electronic Data Processing Audit) / Computer audit merupakan suatu proses dikumpulkannya data dan dievaluasinya bukti untuk menetapkan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian, internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer.

Jenis - Jenis Audit

1. Jenis audit berdasarkan luas pemeriksaan

Pada segi ini, audit bisa dibedakan menjadi:

a. General audit (pemeriksaan umum)

Suatu pemeriksaan umum atas laporan keuangan yang dilakukan oleh

Kantor Akuntan Publik (KAP) independen dengan tujuan untuk bisa memberikan pendapat mengenai kewajaran laporan keuangan secara keseluruhan. Pemeriksa tersebut harus dilakukan sesuai dengan standar profesional akuntan publik dan memperhatikan kode etik akuntan Indonesia, aturan etika KAP yang telah disahkan oleh Ikatan Akuntan Indonesia serta standar pengendalian mutu.

b. Special audit (pemeriksaan khusus)

Suatu pemeriksaan terbatas yang dilakukan oleh KAP yang independen, dan pada akhir pemeriksaan auditor tidak perlu memberikan pendapat terhadap kewajaran laporan keuangan secara keseluruhan. Pendapat yang diberikan terbatas pada pos masalah atau masalah tertentu yang diperiksa. Karena prosedur audit yang dilakukan juga terbatas.

2. Tiga Jenis Manajemen Audit
berdasar keragaman departemen

a. Internal Audit.

Management audit ini dapat dilakukan oleh perusahaan atau departemen yang bersangkutan dgn sistem-sistem prosedur-prosedur atau fasilitas-fasilitas. Auditor yang mengerjakan dapat dari perusahaan mereka sendiri (internal auditor) atau dengan menggaji auditor dari luar perusahaan (external auditor). Internal audit merupakan teknik dimana manajemen dapat merasakan masalah mereka sendiri dan menilai kinerja organisasi kebutuhan titik kekuatan dan kelemahannya. Disebutkan bahwa self audit merupakan bagian dari internal audit yg dilakukan oleh individual dalam sistem mereka sendiri prosedur-prosedur dan fasilitas-fasilitas agar dapat menilai kinerja kebutuhan kekuatan dan kelemahannya.

b. External audit.

Management audit ini dilakukan oleh perusahaan terhadap pemasok mereka atau sub pemasok.

Auditor dapat dari auditor internal maupun auditor eksternal. Management audit dikerjakan untuk menilai status kontrak atau perjanjian yang dibuat perusahaan pemasok atau sub pemasok untuk menentukan keadaan perusahaan atas barang yang akan diterima sesuai dengan yang dibayarkannya.

c. Extrinsic Audit Management.

Audit ini dilakukan oleh pelanggan atau badan-badan yang berkaitan dengan peraturan atau suatu agen inspeksi. Audit ini meliputi pelanggan dari perusahaan-perusahaan pemasok dan sub pemasok.

Pembagian jenis audit yang sejenis :

a. Audit Internal

Audit internal adalah sebuah kegiatan yang dirancang untuk menambah nilai dan meningkatkan operasi badan secara independen. Kegunaanya untuk membantu badan mencapai objektif tujuan dengan sistematis, dengan pendekatan terperinci dalam menilai dan meningkatkan efektifitas dari resiko

manajemen, kontrol, dan proses badan organisasi.

Audit internal sebagai perantara untuk meningkatkan keefektifitasan dan keefesienan suatu organisasi dengan menyediakan wawasan dan rekomendasi berdasarkan analisis dan dugaan yang bersumber dari data dan proses usaha. Para auditor internal dikenal sebagai karyawan yang dibentuk untuk melakukan audit internal.[2]

b. Audit eksternal

Pada businessdictionary audit external diartikan sebagai audit yang dilakukan oleh badan(independent) eksternal yang memenuhi syarat-syarat. Yang bertujuan untuk menentukan antara lain, apakah catatan akuntansi itu akurat dan lengkap, apakah disusun sesuai dengan ketentuan PSAK, dan apakah laporan yang disiapkan dari data menyajikan posisi keuangan dan hasil usaha keuangan secara wajar.

3. Audit berdasarkan bidang

a. Audit laporan keuangan

Audit laporan keuangan (financial statement audit), berkaitan dengan kegiatan memperoleh dan mengevaluasi bukti tentang laporan-laporan entitas dengan maksud agar dapat memberikan pendapat apakah laporan-laporan tersebut telah disajikan secara wajar

b. Audit kepatuhan/ketaatan

Audit kepatuhan (compliance audit), berkaitan dengan kegiatan memperoleh dan memeriksa bukti-bukti untuk menetapkan apakah kegiatan keuangan atau operasi suatu entitas telah sesuai dengan persyaratan ketentuan, atau peraturan tertentu.

Audit kepatuhan/ketaatan berfungsi menentukan sejauh mana peraturan, kebijakan, hukum, perjanjian, atau peraturan pemerintah dipatuhi oleh entitas yang sedang diaudit. Sebagai contoh pemeriksaan SPT (Surat Pemberitahuan) individu dan perusahaan oleh kantor pajak untuk kepatuhannya terhadap hukum pajak.

c. Audit operasional

Audit operasional (operational audit), berkaitan dengan kegiatan memperoleh dan mengevaluasi bukti-bukti tentang efisiensi dan efektivitas kegiatan operasi entitas dalam hubungannya dengan pencapaian tujuan tertentu [8]

Audit ini melibatkan pengkajian sistematis atas aktivitas organisasi, atau bagian dari itu, sehubungan dengan penggunaan sumber daya yang efisien dan efektif. Tujuan dari audit operasional adalah untuk menilai kinerja, mengidentifikasi area yang perlu diperbaiki, dan mengembangkan rekomendasi.

d. Audit Forensik

Tujuan dari audit forensik adalah mendeteksi atau mencegah berbagai jenis kecurangan (fraud). Penggunaan auditor untuk melaksanakan audit forensik telah tumbuh pesat. Beberapa contoh di mana audit forensik bisa dilaksanakan termasuk:

- Kecurangan dalam bisnis atau karyawan

- Investigasi kriminal
- Perselisihan pemegang saham dan persekutuan
- Kerugian ekonomi dari suatu bisnis
- Perselisihan pernikahan.

Risiko yang menyebabkan audit gagal

Pengertian Risiko Audit (Audit Risk)

Risiko Audit atau Audit Risk (AR) adalah kemungkinan risiko salahsaji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Mengingat risiko itu maka, auditor harus melakukan pemeriksaan risiko (risk assessment) sebelum menjalankan proses audit, tepatnya pada fase perencanaan audit (audit planning). Tujuannya: Untuk mengukur dan memetakan risiko audit yang mungkin timbul thus bisa menentukan dimana proses pemeriksaan dilaksanakan secara ketat dan dimana agak longgar, dimana

audit penuh (full audit) dan dimana secara acak (random audit).

Jenis-Jenis Resiko Audit

Ada 3 jenis risiko audit yang wajib diuji dan dipertimbangkan oleh seorang auditor sebelum menjalankan proses audit, yaitu: (1) *risiko inherent* (inherent risk), (2) *risiko pengendalian* (control risk) dan (3) *risiko deteksi* (detection risk).

1. *Risiko Inherent – Atau ‘Inherent Risk’ (IR)* adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, entah karena: (a) kompleksitas transaksi dan klas transaksi; atau (b) kompleksitas perhitungan; atau (c) aset yg mudah tercuri/digelapkan; atau (d) ketiadaan informasi yang sifatnya obyektif. Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakukan pencegahan. Bahkan, juga diluar kendali

pihak auditee sendiri. Dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.

2. *Risiko Pengendalian – Atau ‘Control Risk’ (CR)* adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaannya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau. Karakter perusahaan ber CR tinggi, antara lain.
3. *Risiko Deteksi – Atau ‘Detection Risk’ (DR)*, adalah risiko yang bisa timbul akibat kegagalan auditor dalam mendeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). DR ada dalam kendali auditor. Karena DR sepenuhnya ada pada

kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya). Ada 4 faktor yang berpotensi menghasilkan DR yang tinggi, yaitu:

B. PEMBAHASAN / STUDI KASUS

Contoh Studi Kasus Audit Teknologi Informasi adalah : Studi Kasus Audit Teknologi Informasi : Kejahatan Di Dunia Perbankan

JAKARTA – Masyarakat resah melihat kasus pembobolan dana nasabah di bank yang intensitasnya meningkat sejak awal 2011. Kasus-kasus yang terjadi dalam rentang waktu berdekatan ini pun berdampak pada makin kurangnya kepercayaan publik terhadap perbankan.

Dengan begitu, pengamat perbankan Mirza Adityaswara mengatakan, masyarakat akan lebih berhati-hati

menggunakan layanan perbankan setelah mencuatnya kasus-kasus yang terjadi. “Masyarakat yang semula kurang awas, akan lebih waspada,” katanya, Ahad (2/5).

Mirza berpendapat sistem perbankan yang ada saat ini memang belum sempurna. Ini, jelas dia, bukan hanya terlihat dari sisi pegawai bank, melainkan juga nasabah. “Jangan tergoda melakukan penyelewengan,” katanya.

Tony Prasetyantono, pengamat perbankan, mengatakan berkurangnya kepercayaan publik pasti akan terjadi menyusul berbagai kasus tersebut. Namun, nasabah belum sampai pada satu tindakan menarik uangnya besar-besaran. Karena, jelas Tony, nasabah tidak memiliki pilihan lain yang lebih baik untuk menempatkan uangnya.

Sejauh ini, ujar Tony, bank masih dinilai sebagai tempat terbaik menyimpan aset. “Apalagi yang bersifat likuid, seperti rekening giro dan tabungan,” katanya. “Namun, nasabah akan lebih selektif memilih bank.”

Nasabah, lanjut dia, juga akan lebih memantau rekeningnya agar luput dari pembobolan. Tony menilai, kejahatan perbankan yang terjadi belakangan lebih mengarah pada kesalahan kolektif. Penyebabnya, ia menjelaskan, muncul dari sisi perbankan, nasabah, Bank Indonesia, maupun aturan hukumnya.

Tony mencontohkan, bank kerap menyembunyikan penyimpangan karena takut reputasinya rusak, sedangkan nasabah tidak aktif memantau rekening miliknya. Sementara, BI memiliki keterbatasan dalam memantau banyaknya perbankan yang ada di Tanah Air. “Hukuman terhadap pelaku fraud juga kurang maksimal sehingga kurang menimbulkan efek jera,” jelasnya.

Saat ini. Direktorat Kriminal Khusus (Ditkrimsus) Polda Metro Jaya sedang menangani sembilan kasus perbankan sejak Januari 2011. Bulan lalu, dana deposito milik PT Elnusa Rp 111 miliar di Bank Mega dicairkan tanpa seizin manajemen perusahaan tersebut dengan pelaku melibatkan orang dalam bank. Sebelumnya, simpanan nasabah

prioritas Citibank dibobol oleh karyawan bank asing tersebut yang bernama Inong Malinda alias Malinda Dee.

Kepala Bidang Humas Polda Metro Jaya Kombes Baharudin Djafar mengatakan, kasus pembobolan bank tak hanya terjadi di bank swasta. Menurutnya, akhir pekan lalu, bank milik negara pun tak luput dari jarahan oknum pegawainya yang nakal. Dari sembilan kasus perbankan itu, polisi berhasil menangkap 30 tersangkanya.

Kasat Fiskal, Moneter, dan Devisa Ditkrimsus Polda Metro Jaya AKBP Arismunandar menambahkan, kasus pembobolan dana perbankan biasanya melibatkan orang dalam bank. Sementara itu, Corporate Secretary BSB, Evi Yulia Kurniawati, mengatakan pihaknya menjalankan tata tertib sesuai standar dan memperketat kontrol internal agar terhindar dari kejahatan perbankan.

Saran-saran agar kejahatan serupa tidak terulang:

- Dalam kasus diatas sebaiknya para nasabah harus lebih berhati-hati

dan sebaiknya pihak perbankan memberikan penyuluhan kepada para nasabah.

- Selain itu dunia perbankan wajib melakukan edukasi kepada nasabah tentang masalah yang sering terjadi. Edukasi tersebut diberikan setidaknya bagi nasabah baru dalam menggunakan fasilitas perbankan.
- Melakukan perbaikan atas lemahnya sistem keamanan jaringan.
- saatnya otoritas mengurus sistemik real, karena kalau bank saja tidak dipercaya masyarakat krisis akan berlanjut ke masalah krisis perbankan seperti yang ditakutkan sekarang ini.
- Memperkuat infrastruktur perbankan.

C. ID SECURITY

QWTD4452377-ASP-5244107

D. KESIMPULAN

Kesimpulan dari pembahasan di atas ialah bahwa Audit sistem informasi atau Information System Audit disebut juga EDP Audit (Electronic Data Processing Audit) / Computer audit merupakan suatu proses dikumpulkannya data dan dievaluasinya untuk menetapkan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian, internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer.

Jenis - Jenis Audit

1. Jenis audit berdasarkan luas pemeriksaan
 - a. General audit (pemeriksaan umum)
 - b. Special audit (pemeriksaan khusus)
2. Tiga Jenis Manajemen Audit berdasar keragaman departemen
 - a. Internal Audit.

- b. External audit.
- c. Extrinsic Audit Management.

Pembagian jenis audit yang sejenis :

- a. Audit Internal
 - b. Audit eksternal
-
- 3. Audit berdasarkan bidang
 - a. Audit laporan keuangan
 - b. Audit kepatuhan/ketaatan
 - c. Audit operasional
 - d. Audit Forensik

Adapun risiko Audit atau Audit Risk (AR) adalah kemungkinan risiko salahsaji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Mengingat risiko itu maka, auditor harus melakukan pemeriksaan risiko (risk assessment) sebelum menjalankan proses audit, tepatnya pada fase perencanaan audit (audit planning). Tujuannya: Untuk mengukur dan memetakan risiko audit yang mungkin timbul thus bisa menentukan dimana proses pemeriksaan dilaksanakan secara ketat dan dimana agak longgar, dimana

audit penuh (full audit) dan dimana secara acak (random audit).

E. DISKUSI

Hasil diskusi dari pembahasan di atas ialah bahwa Audit sistem informasi atau Information System Audit disebut juga EDP Audit (Electronic Data Processing Audit) / Computer audit merupakan suatu proses dikumpulkannya data dan dievaluasinya bukti untuk menetapkan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian, internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer.

Jenis – Jenis Audit Sistem Informasi

- 1. Jenis audit berdasarkan luas pemeriksaan yaitu General audit

(pemeriksaan umum) dan Special audit (pemeriksaan khusus)

2. Tiga Jenis Manajemen Audit berdasar keragaman departemen yaitu Internal Audit, External audit, dan Extrinsic Audit Management.

Pembagian jenis audit yang sejenis yaitu Audit Internal dan Audit eksternal

3. Audit berdasarkan bidang yaitu Audit laporan keuangan, Audit kepatuhan/ketaatan, Audit operasional, dan Audit Forensik

Adapun risiko Audit atau Audit Risk (AR) adalah kemungkinan risiko salahsaji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Mengingat risiko itu maka, auditor harus melakukan pemeriksaan risiko (risk assessment) sebelum menjalankan proses audit, tepatnya pada fase perencanaan audit (audit planning). Tujuannya: Untuk mengukur dan memetakan risiko audit yang mungkin timbul thus bisa

menentukan dimana proses pemeriksaan dilaksanakan secara ketat dan dimana agak longgar, dimana audit penuh (full audit) dan dimana secara acak (random audit).

F. REFERENCE

- [1] O. M. Febriani and A. S. Putra, "Sistem Informasi Monitoring Inventori Barang Pada Balai Riset Standardisasi Industri Bandar Lampung," *J. Inform.*, vol. 13, no. 1, pp. 90–98, 2014.
- [2] A. S. Putra, "Paperplain: Execution Fundamental Create Application With Borland Delphi 7.0 University Of Mitra Indonesia," 2018.
- [3] A. S. Putra, "2018 Artikel Struktur Data, Audit Dan Jaringan Komputer," 2018.
- [4] A. S. Putra, "ALIAS MANAGER USED IN DATABASE DESKTOP STUDI CASE DB DEMOS."
- [5] A. S. Putra, "COMPREHENSIVE SET OF PROFESSIONAL FOR DISTRIBUTE COMPUTING."
- [6] A. S. Putra, "DATA ORIENTED RECOGNITION IN BORLAND DELPHI 7.0."
- [7] A. S. Putra, "EMBARCADERO DELPHI XE 2 IN GPU-POWERED FIREMONKEY APPLICATION."
- [8] A. S. Putra, "HAK ATAS KEKAYAAN INTELEKTUAL DALAM DUNIA TEKNOLOGY BERBASIS

- REVOLUSI INDUSTRI 4.0.”
- [9] A. S. Putra, “IMPLEMENTASI PERATURAN PERUNDANGAN UU. NO 31 TAHUN 2000 TENTANG DESAIN INDUSTRI BERBASIS INFORMATION TECHNOLOGY.”
- [10] A. S. Putra, “IMPLEMENTATION OF PARADOX DBASE.”
- [11] A. S. Putra, “IMPLEMENTATION OF TRADE SECRET CASE STUDY SAMSUNG MOBILE PHONE.”
- [12] A. S. Putra, “IMPLEMENTATION PATENT FOR APPLICATION WEB BASED CASE STUDI WWW. PUBLIKLAMPUNG.COM.”
- [13] A. S. Putra, “IMPLEMENTATION SYSTEM FIRST TO INVENT IN DIGITALLY INDUSTRY.”
- [14] A. S. Putra, “MANUAL REPORT & INTEGRATED DEVELOPMENT ENVIRONMENT BORLAND DELPHI 7.0.”
- [15] A. S. Putra, “PATENT AS RELEVAN SUPPORT RESEARCH.”
- [16] A. S. Putra, “PATENT FOR RESEARCH STUDY CASE OF APPLE. Inc.”
- [17] A. S. Putra, “PATENT PROTECTION FOR APPLICATION INVENT.”
- [18] A. S. Putra, “QUICK REPORT IN PROPERTY PROGRAMMING.”
- [19] A. S. Putra, “REVIEW CIRCUIT LAYOUT COMPONENT REQUIREMENT ON ASUS NOTEBOOK.”
- [20] A. S. Putra, “REVIEW TRADEMARK PATENT FOR INDUSTRIAL TECHNOLOGY BASED 4.0.”
- [21] A. S. Putra, “TOOLBAR COMPONENT PALLETTE IN OBJECT ORIENTED PROGRAMMING.”
- [22] A. S. Putra, “WORKING DIRECTORY SET FOR PARADOX 7.”
- [23] A. S. Putra, “ZQUERY CONNECTION IMPLEMENTED PROGRAMMING STUDI CASE PT. BANK BCA Tbk.”
- [24] A. S. Putra, D. R. Aryanti, and I. Hartati, “Metode SAW (Simple Additive Weighting) sebagai Sistem Pendukung Keputusan Guru Berprestasi (Studi Kasus: SMK Global Surya),” in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 85–97.
- [25] A. S. Putra and O. M. Febriani, “Knowledge Management Online Application in PDAM Lampung Province,” in *Prosiding International conference on Information Technology and Business (ICITB)*, 2018, pp. 181–187.
- [26] A. S. Putra, O. M. Febriani, and B. Bachry, “Implementasi Genetic Fuzzy System Untuk Mengidentifikasi Hasil Curian Kendaraan Bermotor Di Polda Lampung,” *SIMADA (Jurnal Sist. Inf. dan Manaj. Basis Data)*, vol. 1, no. 1, pp. 21–30, 2018.

- [27] A. S. Putra, H. Sukri, and K. Zuhri, "Sistem Monitoring Realtime Jaringan Irigasi Desa (JIDES) Dengan Konsep Jaringan Sensor Nirkabel," *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 8, no. 2, pp. 221–232.
- [28] D. P. Sari, O. M. Febriani, and A. S. Putra, "Perancangan Sistem Informasi SDM Berprestasi pada SD Global Surya," in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 289–294.