JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 3, Agustus Tahun 2024
ISSN 3025-0919 (media online)
Hal 453-457

Audit Teknologi Sistem Informasi Di Era Transformasi Digital: Evaluasi Keamanan, Efektivitas, Dan Kepatuhan

Sofyan Mufti Prasetyo[1*], Della Valentina[2], Muhamad Syukron Sobari[3], Muhammad. Fariz[4], Ihsan Albarr[5]

[1,2,3,4,5]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Banten, Indonesia
Email: [1*]dosen01809@unpam.ac.id, [2]dellavlntn655@gmail.com
(* : coressponding author)

Abstrak - Audit sistem informasi adalah proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien. Ada beberapa aspek yang diperiksa pada audit sistem informasi yakni audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, aspek security, audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit sistem informasi sendiri merupakan gabungan dari berbagai macam ilmu, antara lain traditional audit, manajemen sistem informasi, sistem informasi akuntansi, ilmu komputer, dan behavioral science. Standar yang digunakan dalam meng audit sistem informasi adalah standar yang diterbitkan oleh ISACA yaitu ISACA IS Auditing Standard. Selain itu ISACA juga menerbitkan IS Auditing Guidance dan IS Auditing Procedure.

Kata Kunci : Audit Teknologi Sistem Informasi, Integritas Data, ISACA IS Auditing Standard

Abstract - *An information system audit is the process of collecting and assessing evidence to determine whether a computer system can maintain assets, maintain data integrity, achieve organizational goals effectively and use resources efficiently. There are several aspects examined in the audit system, namely the overall audit including effectiveness, efficiency, system availability, reliability, confidentiality and integrity of information, security aspects, audit of processes, program modifications, audit of data sources and data files. The audit information system itself is a combination of various kinds of science, including traditional auditing, management information systems, accounting information systems, computer science, and behavioral science. The standards used in auditing information systems are standards published by ISACA, namely the ISACA IS Auditing Standard. Apart from that, ISACA also publishes IS Auditing Guidance and IS Auditing Procedures.*

Keywords: *Information Systems Technology Audit, Data Integrity, ISACA IS Auditing Standard*

1. PENDAHULUAN

Perkembangan peradaban manusia yang pesat seiring dengan kemajuan ilmu pengetahuan dalam bidang informasi dan komunikasi telah menciptakan berbagai alat dan sistem yang mendukung Teknologi Informasi (TI). Dari sistem komunikasi hingga alat komunikasi interaktif, TI telah merasuki hampir semua bidang dan lapisan masyarakat. Dalam dunia bisnis, dukungan TI memberikan keunggulan kompetitif yang signifikan, terutama dalam mengaudit sistem informasi akuntansi berbasis komputerisasi. Hal ini membantu meningkatkan penyediaan informasi untuk mendukung proses pengambilan keputusan manajemen, baik dalam mengembangkan sistem yang ada maupun menyusun sistem baru, serta dalam perencanaan dan pengendalian operasi perusahaan.

Pengendalian (controlling) merupakan salah satu fungsi penting manajemen dalam mencapai tujuan organisasi, yang berupaya mengurangi risiko kerugian dan penyimpangan. Pengendalian internal yang efektif adalah salah satu faktor kunci kesuksesan sebuah organisasi. Dengan adanya sistem pengendalian internal yang efektif, manajemen dan anggota organisasi dapat memiliki keyakinan yang memadai dalam mencapai tujuan dan sasaran organisasi. Sistem pengendalian internal yang baik membantu dalam mencapai efisiensi, mengurangi risiko kerugian, dan menghasilkan laporan keuangan yang andal dan sesuai dengan hukum serta peraturan yang berlaku.

2. METODE

Dalam penelitian ini, kami menggunakan pendekatan yang sistematis untuk mengaudit Sistem Informasi dan Teknologi Informasi (TI) dalam sebuah organisasi. Metodologi yang

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 3, Agustus Tahun 2024
ISSN 3025-0919 (media online)
Hal 453-457

digunakan terdiri dari beberapa tahap penting, yaitu perencanaan, pelaksanaan, pengumpulan data, analisis, dan pelaporan hasil.

3. ANALISIS DAN PEMBAHASAN

Definisi Audit Sistem Informasi merupakan suatu proses pengumpulan dan pengevaluasian bukti-bukti yang dilakukan oleh pihak yang independen dan kompeten untuk mengetahui apakah suatu sistem informasi dan sumber daya terkait, secara memadai telah dapat digunakan untuk:

a. Melindungi aset

b. Menjaga, integritas dan ketersediaan sistem dan data

c. Menyediakan informasi yang relevan dan handal

d. Mencapai tujuan organisasi dengan efektif

e. Menggunakan sumber daya dengan efisien.

3.1 Tujuan Dan Lingkup Audit Sistem Informasi

Tujuan Audit Sistem Informasi dapat dikelompokkan ke dalam dua aspek utama, yaitu:

1. Conformance (Kesesuaian) Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu :Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan) dan Compliance (Kepatuhan).

b. 2. Performance (Kinerja) Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kinerja, yaitu : Effectiveness (Efektifitas), Efficiency (Efisiensi), Reliability (Kehandalan).

3.2 Tujuan Audit Sistem Informasi

a. Pengamanan aset. Aset informasi suatu perusahaan seperti perangkat keras (hardware), perangkat lunak (*software*), sumber daya manusia, dan data harus dijaga dengan sistem pengendalian intern yang baik agar tidak ada penyalahgunaan aset perusahaan.

b. Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengmbilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut sudah dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan user. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

c. Efisiensi sistem menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memnuhi kebutuhan user dengan sumber daya informasi yang minimal. Cara kerja sistem benar (doing thing right).

d. Ketersediaan (*Availability*)

   Berhubunganketersediaan dukungan/layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara kontinyu terhadap proses bisnis kegiatan perusahaan. Makin sering terjadi gangguan (system down) maka berarti tingkat ketersediaan sistem renda.

e. Kerahasiaaan (*Confidentiality*)

   Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses dari pihak yang idak berwenang.

f. Kehandalan (*Realibility*)

   Berhubungan dengan kesesuaian dan kekuratan bagi manajemen dalam pengolahan organisasi, pelaporan dan pertanggungjawaban.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 3, Agustus Tahun 2024
ISSN 3025-0919 (media online)
Hal 453-457

g. Menjaga integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut seperti kelengkapan kebenaran dan keakuratan.

h. Kerahasiaaan (*Confidentiality*)

Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses dari pihak yang idak berwenang.

i. Kehandalan (*Realibility*)

Berhubungan dengan kesesuaian dan kekuratan bagi manajemen dalam pengolahan organisasi, pelaporan dan pertanggungjawaban.

j. Menjaga integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut seperti kelengkapan kebenaran dan keakuratan.

3.3 Tipe Audit

Audit yang dilaksanakan sesuai tipe perusahaan yaitu operasional, compliance, pengembangan system, internal control, financial dan kecurangan audit. Empat jenis auditor yang dilibatkan dalam menyelenggarakan audit yang di list adalah:

a. Internal auditor adalah karyawan perusahaan,yang pada umumnya melaksanakan compliance,operasional,penge mbangansistem,pengawasan intern&kecurangan audit

b. Ekstenal auditor adalah akuntan publik independen yang ditugaskan oleh perusahaan, secara khusus melaksanakan audit keuangan. Dalam berbagai macam audit keuangan, eksternal auditor dibantu oleh internal auditor. akantetapi auditor eksternal yang bertanggung jawab untuk menegaskan kewajaran laporan keuangan.

c. Goverment auditor,melaksanakan pemenuhan audit/menguji laporan perusahaan atas pengawasan yang menyangkut para pegawai pemerintahan.contoh: pemeriksa bank pemerintahan melaksanakan audit bank,auditor yang dtugaskan oleh auditor negara yang umumnya melaksanakan audit daerah dan para pegawai pemerintah.

d. Fraud auditor, mengkhususkan dalam menyelidiki kecurangan&bekerja secara tertutup dengan internal auditor&pengacara,fraud examminer contoh: kesatuan FBI penyelidikan kecurangan,perusahan besar akuntan publik,IRS,perusahaan asuransi

3.4 Jenis Audit

a. Operational audit, terkonsen pada efisiensi dan efectifitas sumberdaya digunakan untuk melaksanakan tugas, meliputi kesesuaian praktik&prosedur dengan peraturan.

b. Compliance audit terkonsentrasi pada cakupan undang-undang, peraturan pemerintah, pengendalian dan kewajiban badan eksternal lain yang telah diikut.

c. Project manajement&change control audit,(dulu dikenal sebagai suatu pengembangan sistem audit)terkonsentrasi oleh efesiensi&efektifitas pada berbagai tahap pengembangan sistem siklus kehidupan yang sedang diselenggarakan.

d. Internal control audit terkonsentrasi pada evaluasi struktur pengendalian internal.

e. Financial audit terkonsentrasi pada kewajaran laporan keuangan yang menunjukan posisi keuangan, aliran kas dan hasil kinerja perusahaan.

f. Fraud audit adalah nonrecurring audit yang dilaksanakan untuk mengumpulkan bukti untuk menentukan apakah sedang terjadi, telah terjadi atau akan terjadi kecurangan. Dan penyelesaian hal sesuai dengan pemberian tanggung jawab.

3.5 Tahapan Audit

a. Subjek Audit

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 3, Agustus Tahun 2024
ISSN 3025-0919 (media online)
Hal 453-457

Tentukan/identifkasi unit/lokasi yang diaudit. Sasaran audit. Tentukan sistem secra spesifik, fungsi atau unit orgainisasi yang akan diperiksa

b. Jangkauan audit.

Identifikasi sistem secara spesifik, fungsi atau unit organisasi untuk dimasukkan lingkup pemeriksaan.

c. Rencana pre-audit

1) Identifikasi kebutuhan keahlian teknik dan sumber daya yang diperlukan untuk audit
2) Identifikasi sumber bukti untuk tes atau review seperti fungsi flowchart, kebijakan, standard prosedur dan kertas kerja audit sebelumnya.

d. Prosedur audit dan langkalangkah pengumpulann bukti audit.

1) Identifikasi dan pilih pendekatan audit untuk memeriksa dan menguji pengendalian intern
2) Identifikasi daftar individu untuk interview
3) Identifikasi dan menghasilkan kebijakan yang berhubungan dengan bagian, standar dan pedoman untuk interview
4) Mengembangakn instrumen audit dan metodologi pengujian dan pemeriksaan kontrol internal

e. Prosedur untuk evaluasi

1) Organisasikan sesuai kondisi dan situasi
2) Identifikasi prosedur evaluasi atas tes efektifitas dan efisiensi sistem, evaluasi kekuatan dari dokumen, kebijakan dan prosedur yang diaudit

f. Laporan hasil audit. Siapkan laporan yang objektif, konsteuktif (bersifat membangun) dan menampung penjelasan audit.

3.6 Tools yang Digunakan Untuk IT Audit

Tool-Tool Yang Dapat Digunakan Untuk Mempercepat Proses Audit Teknologi Informasi, antara lain:

a. ACL(Audit Command Langu age) merupakan sebuah softw are CAAT (Computer Assiste d Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber

b. Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber.

c. Powertech Compliance Assessment merupakan automated audit tool yang dapat dipergunakan untuk mengaudit dan mem-benchmark user access to data, public authority to libraries, user security, system security, system auditing da n administrator rights (speci al authority) sebuah server AS/400.

d. Nipper merupakan audit auto mation software yang dapat dipergunakan untuk mengaudi t dan mem- benchmark konfigurasi sebuah router.

e. Nessus merupakan sebuah vulnerability assessment software.

f. Metasploit Framework merupakan sebuah penetration testing tool.

g. NMAP merupakan open source utility untuk melakukan security auditing.

h. Wireshark merupakan network utility yang dapat dipergunakan untuk meng-capture paket data yang ada di dalam jaringan komputer.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 3, Agustus Tahun 2024
ISSN 3025-0919 (media online)
Hal 453-457

4. KESIMPULAN

Audit Sistem Informasi merupakan suatu proses pengumpulan & pengevaluasian bukti-bukti yang dilakukan oleh pihak yang independen & kompeten untuk mengetahui apakah suatu sistem informasi dan sumber daya terkait, secara memadai telah dapat digunakan untuk: melindungi aset, menjaga integritas & ketersediaan sistem & data, menyediakan informasi yang relevan & handal, mencapai tujuan organisasi dengan efektif, menggunakan sumber daya dengan efisien, sistem informasi menyiratkan penggunaan teknologi komputer dalam suatu organisasi untuk menyediakan informasi bagi pengguna. Sistem informasi berbasiskomputer merupakansatu rangkaian perangkat lunak & perangkat lunak yang dirancang untuk mentransformasi data menjadi informasi yang berguna, secara memadai dapat digunakan untuk:

a. Melindungi aset
b. Menjaga integritas dan ketersediaan sistem dan data
c. Menyediakan informasi yang relevan dan handal
d. Mencapai tujuan organisasi dengan efektif
e. Menggunakan sumber daya dengan efisien.

REFERENCES

ISACA. (2014). *IS Auditing Standard*. ISACA.
Romney, M. B., & Steinbart, P. J. (2014). *Accounting Information Systems* (13th ed.). Pearson.
Bodnar, G. H., & Hopwood, W. S. (2013). *Accounting Information Systems* (11th ed.). Pearson.
Laudon, K. C., & Laudon, J. P. (2016). *Management Information Systems: Managing the Digital Firm* (14th ed.). Pearson.
Hall, J. A. (2015). *Accounting Information Systems* (9th ed.). Cengage Learning.
Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
Gordon, L. A., & Loeb, M. P. (2002). *The Economics of Information Security Investment*. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.
Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. John Wiley & Sons.
Parker, D. B. (2007). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Wiley.
Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30.
Stallings, W., & Brown, L. (2015). *Computer Security: Principles and Practice* (3rd ed.). Pearson.
Leitch, M., & Warren, M. (2011). *Information Security Management Handbook*. CRC Press.
Debreceny, R. S., & Gray, G. L. (2011). *IT Governance and Internal Audits*. The CPA Journal, 81(8), 62-64.
Rezaee, Z. (2002). *Financial Statement Fraud: Prevention and Detection*. John Wiley & Sons.
Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.
Wallace, P. (2015). *Information Systems in Today's Business Environment*. Wiley.
Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Wiley.
Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). *Structures, Processes, and Relational Mechanisms for IT Governance: Theories and Practices*. Idea Group Publishing.
Johnson, E. C. (2006). *Security Awareness: Applying Practical Security in Your World*. Elsevier.
Ross, S. (2015). *Systemic Risk in the Financial System: A Look at the Role of Financial and Non-Financial Institutions in the 2007-2008 Credit Crisis*. CFA Institute.