JURNAL RISET AKUNTANSI DAN BISNIS

VOLUME 2 NO 2
JULI 2016

Jurnalakuntansi.lp3ibdg@gmail.com

AUDIT SISTEM INFORMASI DAN PERAN AUDITOR

Mumu Muzaemi – Dosen Tetap Prodi Akuntansi Politeknik LP3I Bandung (mumu.zaeni@gmail.com)

ABSTRACT

Information system auditing is intended to collect and evaluate evidences to know if a computer system is able to safeguard assets and maintain data integrity so that the goals of organization can be reached effectively and efficiently. The auditors can audit using three approaches such as audit around the computer; audit through the computer and audit with the computer. In addition, Auditors should consider the risks and related controls mainly general control and application control.

Audit techniques which can be applied include integrated test facility, embedded audit routine, extended record, snapshot, control flowcharting, mapping, and using audit software such as ACL, IDEA, Microsoft Excel or Microsoft Access. In this context, auditors are required to improve their skills related to information technology.

***KeyWords** : auditing, information system, auditor, safeguard assets, maintain data, efficient, effective, risk, general control, application control, ACL, IDEA*

.

PENDAHULUAN

Latar Belakang

Saat ini banyak perusahaan yang telah melakukan komputerisasi untuk aplikasi akuntansi, ada yang telah menerapkan secara terintegrasi maupun hanya per modul aplikasi akuntansi tertentu misalnya aplikasi *general ledger*, aplikasi penjualan, aplikasi penggajian, aplikasi kas dan bank, aplikasi pembelian dan aplikasi akuntansi lainnya. Herwati (2008) meneliti penerapan audit sistem informasi persediaan menyimpulkan bahwa aplikasi sistem informasi persediaan telah memadai dengan memberikan informasi yang andal dan tepat waktu sehingga mempermudah manajemen dalam pengambilan keputusan di bidang persediaan. Penelitian mengenai aplikasi persediaan juga dilakukan oleh Noerlina (2008), yang menyarankan agar kelemahan sistem persediaan dapat segera dilakukan. Banyak perusahaan berskala kecil maupun menengah mengambil keputusan untuk melakukan komputerisasi karena investasinya relatif murah, dan piranti lunaknya sudah tersedia banyak di pasar baik yang sifatnya *general* maupun

customized, dan teknologi komunikasinya sangat mendukung untuk melakukan integrasi dengan membangun jaringan (*networking*) atau berbasis web. Software Myob, Accurate merupakan contoh piranti lunak akuntansi yang tersedia banyak di pasar. Pada beberapa perusahaan multi nasional bahkan sudah menerapkan ERP (*Enterprises Resource Planning*) seperti PT Sampoerna, PT Telkom, Pertamina.

Akuntansi yang telah diolah secara *computerized* ini akan berdampak besar terhadap aktivitas di bidang auditing. Auditing untuk perusahaan yang sudah melakukan komputerisasi di bidang akuntansi, berbeda perlakuannya untuk perusahaan yang belum menerapkan komputer dalam aktivitas bisnisnya. Menurut Fefri (2007), teknologi informasi akan berimplikasi pada proses audit, pembelajaran auditing dan berimplikasi juga pada auditor. Teknologi informasi akan mempengaruhi proses audit. Auditor yang peduli dengan penggunaan TI dalam pekerjaannya akan memetik manfaat karena dapat bekerja lebih efektif dan efisien

Audit sistem informasi (TI) dapat juga diterapkan pada instansi pemerintah seperti penelitian yang dilakukan oleh Setiawan dan Mustofa (2013), teknologi informasi mendukung keberhasilan pengelolaan di instansi pemerintah dengan cara meningkatkan efisiensi dan efektivitas tatakelola TI. Pemerintah dapat mengadopsi *best practices* dengan memanfaatkan COSO, COBIT, ITIL, IT *Security*, *National Institute of Standards and Technology* (NIST), *British Standard Institution* (BSI) *Baselines*, ISO/IEC 27002, ISO / IEC 385000, dan lain-lain. Penelitian yang serupa juga dilakukan oleh Widayanti dan Purnamawati (2013) yang mengaudit aplikasi sistem manajemen pemeriksaan (SMP) Badan Pemeriksa Keuangan Republik Indonesia dengan kesimpulan bahwa pengendalian Biro TI sudah berjalan dengan baik.

Tulisan ini menjelaskan lebih lanjut mengenai aktivitas audit sistem informasi; mengapa harus menggunakan COBIT ? Mengapa harus dilakukan audit sistem informasi? Teknik audit apa saja yang dapat diterapkan? Bagaimana peran auditor di dalamnya?

LANDASAN TEORI

Definisi Audit

Arens *et.al*. (2009) mendefinisikan *auditing* sebagai berikut : "*Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person*." (Pengumpulan dan penilaian bukti mengenai informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi tersebut dan kriteria yang ditetapkan. Auditing harus dilakukan oleh orang yang kompeten dan independen).

Dari definisi di atas, auditing memiliki karakteristik tertentu yaitu : (a). ada kriteria atau standar yang digunakan untuk menguji asersi dan informasi contohnya adalah SAK (Standar Akuntansi Keuangan); (b). aktivitas mengumpulkan dan mengevaluasi bukti; (c). independensi dan kompetisi auditor; (d). pelaporan audit.

Akuntan Publik (Kantor Akuntan Publik) yang melakukan audit dan *auditee*-nya memproses data akuntansinya berbasis komputer, dapat menggunakan dua pendekatan : *audit around the computer* dan *audit through the computer*.

Pada audit *around the computer* (audit di sekitar komputer), auditor memanfaatkan *hard copy* yang dihasilkan oleh sistem komputer berbentuk input dan output, tanpa melakukan pengujian (*test*) pada sistem komputer. Wicaksono (2014) melakukan audit terhadap

pengendalian umum dan pengendalian aplikasi pada PT Lagio Furniture dengan pendekatan *audit around the computer*, menyarankan kepada pihak perusahaan untuk memperhatikan aspek keamanan (*security*) dan input.

Pada audit *through the computer* (audit melalui komputer), di samping auditor memeriksa input dan outputnya, auditor juga melakukan pengujian pada sistem komputernya. Pengujian tersebut merupakan *compliance test* yang dapat dilakukan menggunakan *Generalized Audit Software* (GAS) dan memasukkan data palsu (*dummy data*) untuk mengetahui apakah data tersebut diproses sesuai dengan apa yang seharusnya. *Dummy* data digunakan agar tidak mengganggu data aslinya. Untuk memenuhi tugas ini, KAP harus memiliki *computer audit specialist* yang merupakan auditor yang sudah berpengalaman di bidang audit sistem informasi dan bergelar CISA *(Certified Information System Auditor*). Menurut penelitian Sasongko (2002), dengan sampel 245 KAP, ternyata tidak sampai 10% Kantor Akuntan Publik (KAP) yang menerapkan audit sistem informasi dalam proses auditnya.

Opini yang dapat diberikan oleh auditor eksternal, yaitu : (1). *Unqualified opinion* (pendapat wajar tanpa pengecualian); (2). *Unqualified opinion with explanatory language* (pendapat wajar tanpa pengecualian dengan tambahan bahan penjelasan); (3). *Qualified opinion* (pendapat wajar dengan pengecualian); (4). *Adverse opinion* (pendapat tidak wajar); (5). *Disclaimer of opinion* (tidak memberikan pendapat).

Definisi Audit Sistem Informasi

Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safegurds assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. (Ron Weber, 1999 : 10). Audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah sebuah sistem komputer melindungi aset, menjaga integritas data, memungkinkan tujuan organisasi dapat dicapai secara efektif, dan penggunaan sumber daya secara efisien.

Tujuan audit sistem informasi adalah : (a). menjaga aset TI, misalnya perangkat keras, perangkat lunak, orang, data, berkas (file), sistem dokumentasi, dan perlengkapan (barang habis pakai); (b). memelihara integritas data agar memenuhi syarat kelengkapan, akurat. Hal ini merupakan upaya untuk meminimalisir faktor-faktor ketidakpastian pada penggunaan informasi hasil sistem IT; (c). meningkatkan efektivitas dan efisiensi sistem informasi.

Pada audit sistem informasi ini, *auditee*-nya adalah divisi / departemen IT, standar yang digunakan adalah COBIT (*Control Objectives for Information and related Technology*), asosiasinya adalah ISACA (*Information System Audit and Control Association*), kualifikasinya adalah CISA (*Certified Information System Auditor*).

Jenis-Jenis Audit

Secara garis besar, audit dapat dikelompokkan menjadi 3 yaitu : audit laporan keuangan; audit operasional; dan audit ketaatan. Tujuan audit laporan keuangan adalah untuk menentukan kewajaran laporan keuangan, asersinya adalah informasi dalam laporan keuangan, kriteria yang digunakan adalah prinsip akuntansi yang berlaku umum (standar akuntansi), outputnya adalah opini auditor, auditornya adalah akuntan publik (auditor ekstern). Tujuan audit operasional adalah menilai efisiensi, efektivitas, ekonomis operasi suatu entitas, asersinya adalah kinerja (data operasional), kriterianya bervariasi tergantung visi/misi, standar operasi entitas, outputnya

pernyataan mengenai efektivitas, efisiensi, ekonomis dan rekomendasi perbaikan, auditornya adalah auditor (intern, ekstern, pemerintah). Tujuan audit ketaatan adalah untuk menentukan kepatuhan auditan (*auditee*) pada kebijakan, peraturan atau prosedur, asersinya adalah data mengenai pelaksanaan kebijakan, peraturan-peraturan, prosedur, kriterianya adalah kebijakan, peraturan, prosedur yang ditetapkan misalnya undang-undang perpajakan, undang-undang ketenagakerjaan, outputnya adalah pernyataan temuan atau tingkat kepatuhan, auditor yang terlibat adalah auditor intern, auditor pemerintah, akuntan publik (auditor ekstern).

Pengendalian dalam Sistem Informasi

Instansi pemerintah dan swasta di Indonesia pada umumnya masih menggunakan pengendalian intern menurut konsep COSO (the Committee of Sponsoring Organizations of the Treadway Commission) yaitu "*a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations*" (suatu proses yang dipengaruhi oleh dewan direksi, manajemen, dan personil lainnya, dirancang untuk memberikan jaminan yang memadai untuk mencapai efektivitas dan efisiensi operasi, keandalan laporan keuangan, dan ketaatan terhadap hukum yang berlaku dan peraturan).

Menurut Tuanakotta (2013:126-145) *internal control* dirancang, diimplementasikan, dan dipelihara oleh TCWG (*Those Charge With Governance*), manajemen, dan karyawan lain untuk menangani risiko bisnis dan risiko kecurangan yang diketahui (*identified business and fraud risks*) mengancam pencapaian tujuan entitas, seperti pelaporan keuangan yang andal. Pengendalian selalu merupakan jawaban (*response*) untuk menangkal (*mitigate*) suatu ancaman (kemungkinan terjadinya risiko). Pengendalian yang tidak merupakan jawaban untuk menangkal ancaman adalah kesia-siaan (*redundant*). Langkah pertama dalam mengevaluasi rancangan pengendalian adalah tentukan risiko apa yang perlu ditangkal. Langkah kedua, tentukan pengendalian yang ada untuk menangkal risiko tersebut.

Unsur atau komponen pengendalian COSO meliputi : (1). lingkungan pengendalian; (2). penaksiran risiko; (3). aktivitas pengendalian; (4). informasi dan komunikasi; dan (5). pemantauan. Tujuan pengendalian intern adalah untuk meningkatkan : (1). efisiensi dan efektivitas operasi; (2). keandalan laporan keuangan; dan (3). ketaatan kepada hukum yang berlaku dan peraturan.

Lingkungan pengendalian mencakup keteladanan pimpinan puncak dan kepeduliannya terhadap pengendalian. Keteladanan dimanifestasikan dalam bentuk integritas, filosofi dan gaya kepemimpinan, sedangkan kepedulian terhadap pengendalian diwujudkan dalam struktur organisasi yang memadai, pelimpahan wewenang dan tanggungjawab, pedoman pengendalian, prosedur kerja.

Penaksiran risiko dilaksanakan oleh manajemen secara terus menerus dengan mengidentifikasi risiko, mengukur signifikansi dan kemungkinan terjadinya, serta melakukan tindakan untuk menghilangkan atau mengurangi akibat yang merugikan dari risiko tersebut. Pada organisasi berukuran besar, risiko ini ditangani dengan membentuk satu divisi atau bagian tersendiri, sedangkan pada organisasi berukuran sedang dan kecil hal ini dilakukan oleh manajemen puncak atau dilimpahkan pada divisi atau bagian yang sudah ada, seperti bagian pemeriksaan intern (Akmal dan Hadi, 2010 : 4).

Aktivitas pengendalian dibagi menjadi dua yaitu aktivitas yang berhubungan dengan laporan keuangan dan aktivitas yang terkait dengan pengolahan informasi. Aktivitas ini meliputi kegiatan *review* kinerja, pengendalian fisik, pemisahan tugas, dan pengendalian pengolahan informasi yang berbentuk *general control* dan *application control*.

Informasi dan komunikasi mencakup aktivitas untuk mengidentifikasi dan mengolah informasi yang terkait dengan laporan keuangan dan bentuk komunikasi dalam format yang sesuai.

Pemantauan meliputi kegiatan yang dilakukan secara terus menerus seperti pemeriksaan secara fisik, pemeriksaan secara mendadak, dan aktivitas audit yang dilakukan baik oleh auditor intern maupun auditor ekstern.

Berdasarkan pelaku, pengendalian dapat dibagi menjadi tiga yaitu : (a). pengendalian preventif; (b). pengendalian detektif; dan (3). pengendalian korektif. Pengendalian preventif adalah pengendalian yang bersifat mencegah sebelum terjadi yaitu mencegah kesalahan yang tidak disengaja (*error*), kesalahan yang disengaja (*fraud*), memprediksi masalah potensial sebelum terjadi. Pengendalian detektif bersifat aktif yaitu menentukan kapan suatu kejadian yang tidak diinginkan terjadi dan membuat laporan. Pengendalian korektif ditujukan untuk meminimalisir dampak dari sebuah ancaman; memperbaiki masalah yang ditemukan oleh pengendalian detektif; mengidentifikasi masalah; memperbaiki atau mengoreksi kesalahan yang muncul; memodifikasi sistem pengolahan untuk meminimalisir kejadian di masa yang akan datang (Widjaja Tunggal, 2001 : 25).

Pengendalian Umum dan Pengendalian Aplikasi

Menurut Christiawan (2000), *Electronic Data Processing* (EDP) mempengaruhi auditor dalam melakukan pengujian dan jejak audit sehingga perlu dilakukan pengendalian tambahan yaitu pengendalian umum dan pengendalian aplikasi. Pengendalian umum (*general control*) adalah pengendalian yang berkaitan dengan personil, *hardware*, dan lingkungannya. Unsur-unsur yang ada di dalamnya antara lain adanya struktur organisasi yang memadai dan memenuhi kaidah pengendalian; adanya pemisahan fungsi yang tegas antara administrator, analisis sistem, *programmer*, *librarian*, dan operator; adanya rencana kerja dan prosedur kerja yang harus diikuti oleh setiap pimpinan, petugas atau pegawai; adanya pembatasan akses pegawai di bagian komputer dan akses pegawai di luar bagian komputer, seperti kunci masuk ruangan dan *password*; pengendalian *backup* data dan aplikasi. Pengendalian aplikasi digolongkan menjadi tiga, yaitu : (1). Pengendalian masukan, pengendalian yang ditujukan pada semua data yang dimasukkan (*entry*) apakah sudah sah, lengkap, tidak terduplikasi, dan cermat. Pengendalian ini sangat penting karena kesalahan pada saat entri data akan mempengaruhi hasil (output) yang akan digunakan oleh para pengguna informasi; (2). Pengendalian proses yaitu pengendalian untuk mengetahui apakah proses telah dilakukan secara benar, diproses hanya sekali atau sesuai dengan instruksi, dan diproses secara cermat. Biasanya pengendalian ini tersedia (*built-up*) dalam aplikasi yang digunakan; (3). Pengendalian hasil proses yaitu pengendalian untuk mengetahui apakah hasil proses sudah sah, lengkap, cermat, dan diberikan kepada penerima yang berhak.

Risiko dan Risiko Audit

Menurut *International Standard Organization* (ISO), risiko adalah potensi yang akan mengancam hilang atau rusaknya aset. Risiko dalam audit dapat dibagi menjadi tiga, yaitu : (1).

inherent risk (risiko melekat); (2). *control risk* (risiko pengendalian); (3). *detection risk* (risiko deteksi); (4). *Acceptable risk* (risiko yang dapat diterima).

Risiko melekat adalah risiko yang sudah ada pada suatu aktivitas operasi sebelum ada pengendalian intern (manajemen). Risiko pengendalian adalah risiko yang mungkin ada yang tidak dapat ditemukan oleh adanya sistem pengendalian intern (manajemen). Risiko deteksi adalah risiko tidak terdeteksinya suatu salah saji material yang ada. Besar sampel yang ditetapkan akan berbanding terbalik dengan besarnya risiko deteksi. Risiko audit yang dapat diterima adalah kesediaan auditor menerima risiko dari audit yang dilakukannya, biasanya ditetapkan rendah supaya diperoleh risiko yang lebih rendah, dengan demikian akan ditetapkan risiko deteksi yang lebih rendah pula dan besar sampel yang lebih besar. Risiko deteksi = { risiko yang dapat diterima / (risiko bawaaan x risiko pengendalian)}. Sebagai contoh, risiko yang dapat diterima = 0,05, risiko bawaan = 0,30, dan risiko pengendalian = 0,90 maka risiko deteksi = 0,05 / (0,30 x 0,90) = 0,18. Risiko yang dapat diterima =0,20, risiko bawaan = 0,30, dan risiko pengendalian = 0,90, maka risiko deteksinya = 0,20 / (0.30 x 0,90) = 0,74.

PEMBAHASAN

Aktivitas Audit Sistem Informasi

Audit merupakan proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti untuk memberikan asersi berdasarkan kriteria tertentu dan mengkomunikasikan hasilnya kepada pihak yang terkait.

Audit Sistem Informasi (SI) merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan dapat melindungi aset perusahaan, menjaga integritas data, membantu pencapaian tujuan organisasi secara efektif dan dapat menggunakan sumber daya secara efisien. Aktivitas Audit SI atau TI masih relatif baru dibandingkan dengan audit finansial. Ada beberapa aspek yang diperiksa yaitu audit secara keseluruhan menyangkut efektivitas, efisiensi, ketersediaan sistem (*availability system*), keandalan (*reliability*), keyakinan (*confidentiality*), dan integritas (*integrity*), serta keamanan (*security*). Audit TI merupakan kombinasi dari berbagai disiplin ilmu antara lain audit tradisional, manajemen sistem informasi, sistem informasi akuntansi, ilmu komputer, dan ilmu perilaku.

Tahap awal audit sistem informasi adalah perencanaan yang akan menghasilkan suatu program audit. Agar pelaksanaannya dapat berjalan secara efektif dan efisien, auditornya harus orang-orang yang kompeten dan dapat diselesaikan dalam waktu yang disepakati. Pada tahap perencanaan, aspek pengendalian intern perlu dinilai untuk menentukan luasnya pemeriksaan dan akan terlihat pada audit program. Tahap berikutnya adalah mengumpulkan bukti (*evidence*) dan mendokumentasikan bukti serta mendiskusikan dengan *auditee* jika ada temuan (*findings*), dan tahap terakhir adalah membuat laporan audit.

Teknik yang dapat digunakan oleh auditor TI untuk mengumpulkan bukti-bukti antara lain survei, *interview*, observasi, dan *review* dokumentasi termasuk *review source-code*. Dalam proses pengumpulan bukti ini ada beberapa cara yang dapat ditempuh oleh auditor TI yaitu *audit around the computer*, *audit through the computer*, dan *audit with the computer*. Jika *auditee* sudah memanfaatkan *high technology*, audit yang cocok adalah audit *with the computer* atau disebut CAAT (*Computer Aided Auditing Technique*), teknik audit berbantuan komputer. Teknik

ini digunakan untuk menganalisis data, misalnya data transaksi penjualan, pembelian, persediaan, piutang, utang, dan lain-lainnya. Untuk aspek keamanan (*security*), auditor dituntut memiliki keahlian teknis yang memadai.

Standar yang digunakan untuk audit sistem informasi adalah standar yang diterbitkan oleh ISACA (*Information System Audit and Control Association*), yaitu ISACA IS *Auditing Standard*. ISACA juga menerbitkan IS *Auditing Guidance* dan IS *Auditing Procedure*. Standar adalah sesuatu yang harus dipenuhi oleh Auditor SI. *Guidelines* memberikan penjelasan bagaimana auditor dapat memenuhi standar dalam berbagai penugasan audit, dan memberikan langkah-langkah agar sesuai dengan standar. Auditor SI harus dapat menerapkan kemahiran profesionalnya ketika menggunakan *guidance* dan *procedure* (Agoes dan Hoesada, 2012 : 227).

Ada 11 standar untuk audit TI yaitu : (1). *Audit charter*; (2). *Independent audit*; (3). *Profesional Ethic and standard*; (4). *Profesional competence*; (5). *Planning*; (6). *Performance of Audit Work*; (7). *Reporting*; (8). *Follow-Up Activity*; (9). *Irregularities and Irregular Act*, (10). *IT Governance*, dan (11). *Use of Risk Assesment in Audit Planning.* IS *Auditing Guideline* terdiri dari 32 *guidance* dalam mengaudit TI yang mencakup petunjuk untuk mengaudit area-area penting. IS Audit *Procedure* terdiri dari 9 prosedur yang menunjukkan tahap-tahap yang harus dilakukan oleh auditor dalam penugasan audit spesifik, seperti prosedur melakukan *risk assesment*, menguji *instruction detection system*, menganalisis *firewall*, dan sebagainya. Standar dari ISACA setara dengan Standar Profesional Akuntan Publik (SPAP) yaitu menyangkut tatacara pelaksanaan audit. Standar khusus yang digunakan auditor TI adalah COBIT.

COBIT

COBIT (*Control Objective for Information Related Technology*) dikembangkan sebagai suatu *generally applicable and accepted standard for good information Technology* (IT) *security and control practices*. Istilah *generally applicable and accepted* digunakan secara eksplisit dalam pengertian yang sama seperti *Generally Accepted Accounting Principles* (GAAP).

COBIT mengarahkan praktik pengendalian yang baik berdasarkan kewenangan, kerangka pemrosesan, dan aktivitas yang ada dalam suatu struktur yang rasional. COBIT merupakan milik ITGI (*Information Technology Governance Institute*) yang tujuannya untuk membantu pekerjaan para pimpinan pengelola teknologi informasi (CIO).

Banyak perusahaan yang menerapkan teknologi informasi untuk meningkatkan kinerja organisasi apalagi dalam masyarakat global seperti sekarang ini, informasi berpindah tanpa kendala waktu, jarak dan kecepatan. Bagi beberapa perusahaan, informasi dan teknologi merupakan aset perusahaan yang akan mendukung keberadaan organisasi. Ketergantungan perusahaan atau organisasi pada teknologi informasi mengharuskan pihak manajemen mengelola teknologi informasi dengan mengendalikan risiko yang akan terjadi. Hal ini merupakan salah satu kunci keberhasilan penerapan tata kelola yang baik (*good governance*). Tata kelola yang baik merupakan tanggung jawab para pelaksana dan pimpinan organisasi yang di dalamnya menyangkut kepemimpinan, struktur organisasi, dan proses yang menjamin bahwa teknologi informasi pada suatu organisasi menopang serta memperluas strategi dan tujuan organisasi.

Tata kelola Teknologi Informasi (TI) yang baik akan mengintegrasikan dan melembagakan praktik-praktik yang sehat untuk memastikan bahwa teknologi informasi yang ada di dalam perusahaan atau organisasi telah mendukung tujuan organisasi. Organisasi dapat memperoleh manfaat keberadaan informasi dan teknologi informasi yang baik dengan memaksimalkan kelebihan TI, memanfaat kesempatan, dan mengambil keuntungan. Agar

manfaat dapat diperoleh, diperlukan suatu kerangka pengendalian TI yang selaras dan mendukung kerangka pengendalian intern COSO. Kerangka pengendalian TI harus diterima secara luas oleh organisasi untuk meningkatkan kepatuhan dan kepentingan manajemen risiko.

Informasi organisasi harus cukup berkualitas, dapat dipercaya, dan aman. Manajemen harus bersikap optimis dalam memanfaatkan sumber daya yang tersedia seperti aplikasi, informasi, prasarana, dan orang. COBIT terdiri dari 34 tujuan pengawasan tingkat tinggi yang menggambarkan proses TI yang terdiri dari 4 domain yaitu *Plan and Organise*, *Acquire and Implement*, *Deliver and Support*, serta *Monitor and Evaluate*. Dengan mengendalikan 34 tujuan tersebut, organisasi dapat memperoleh keyakinan mengenai kelayakan tata kelola dan pengendalian yang diperlukan untuk lingkungan TI. Untuk mendukung IT *process* tersebut, masih ada sekitar 215 tujuan pengendalian yang lebih detil untuk menjamin kelengkapan dan efektivitas implementasi. Julisar (2010) meneliti mengenai IT *governance*, menyimpulkan bahwa COBIT dengan 4 domainnya dapat dijadikan pedoman bagi manajemen perusahaan untuk memperbaiki IT *governance* di masa mendatang.

Suatu perencanaan audit IT dapat dimulai dengan menentukan area-area yang relevan dan berisiko paling tinggi menggunakan analisis dari 34 proses. Sedangkan kebutuhan dalam penugasan tertentu, misalnya audit proyek TI dapat dimulai dengan memilih proses yang relevan dari proses-proses yang tersedia.

Mengapa harus dilakukan Audit Sistem Informasi ?

Menurut Agoes dan Hoesada (2012 : 229), audit sistem informasi atau teknologi informasi (TI) merupakan aktivitas pengujian pengendalian unit infrastruktur sebuah sistem atau teknologi informasi. Pengujian atau evaluasi tersebut dapat dilakukan dalam bentuk audit keuangan, audit intern. Untuk mengetahui perlu atau tidaknya audit TI, perlu dilihat latar belakang sejarahnya. Sejak tahun 1977, aturan mengenai audit TI sudah dibentuk di Amerika Serikat yang melahirkan beberapa aturan seperti The Gramm Leach Bliley Act, The Sarbanes-Oxley Act, The Health Insurance Portability and Accountability Act, The London Stock Exchange Combines Code, King II dan The Foreign Corrupt Practices Act.

Implementasi TI merupakan hal yang sangat penting bagi sebuah organisasi yang sudah menerapkan sistem informasi yang berbasis komputer atau TI. Perusahaan mulai mempertimbangkan untuk melakukan audit TI karena investasinya termasuk besar, sementara hasilnya sulit diukur. Dalam banyak kasus, kebanyakan manajer TI atau personil TI tidak dapat menjelaskan secara baik dengan pendekatan kuantitatif mengenai investasi yang tercermin dalam ROI (*Return on Investment*). Profesional TI menganggap investasi TI sebagai sesuatu yang *intangible*.

Kegagalan bagian TI dalam menjelaskan manfaat investasi TI; kurang selarasnya kegiatan bagian TI dengan tujuan bisnis perusahaan; investasi di bidang TI yang cenderung membesar; masalah *security* dan *confidentiality* mendorong manajemen puncak untuk mengaudit TI.

Tujuan audit TI adalah untuk mengevaluasi dan memperbaiki efektivitas manajemen risiko, pengendalian, dan tata kelola yang baik (*good governance*). Pentingnya audit TI sejalan dengan kepentingan pencapaian tujuan perusahaan. Perusahaan ingin mengelola berbagai risiko yang terjadi. Kebanyakan perusahaan menolak untuk melakukan audit TI karena merasa yakin bahwa perencanaan investasi di bidang TI sudah benar, di samping karena pertimbangan biaya. Pada prinsipnya, audit TI hampir sama dengan audit keuangan. Audit keuangan merupakan

keharusan, audit TI dilakukan sejauh diperlukan. Pihak yang mendapatkan manfaat dari audit TI adalah perusahaan karena perusahaan dapat mengetahui sampai sejauh mana manfaat TI bagi peningkatan kinerja dan tujuan perusahaan.

Ron Weber (2000 : 5) memberikan beberapa alasan mengapa audit TI harus dilakukan : (1). *organizational costs of data loss*; (2). *cost of incorrect decision making*; (3). *cost of computer abuse*; (4). *value of hardware, software, personnel*; (5). *high costs of computer error*; (6). *maintenance of privacy*; (7). *controlled evolution of computer use*.

1. Kerugian akibat kehilangan data
   Data dapat hilang karena perangkat kerasnya (*hard disk, server*, komputer) rusak atau karena *software*-nya terserang oleh virus sehingga *database*-nya ikut rusak atau karena kebakaran. Untuk memperbaiki data yang rusak atau hilang dapat dilakukan dengan *software-recovery*, tetapi peluang keberhasilannya tidak bisa ditentukan. Bagaimana kalau data tersebut berhubungan dengan pelanggan (nasabah) di sebuah bank, berapa kerugian yang diderita perusahaan akibat musibah tersebut dan kerugian akibat *customer* (nasabah) yang tidak puas atas pelayanannya.
2. Kesalahan dalam pengambilan keputusan
   Ada *adagium* yang populer dalam TI yaitu "*garbage-in garbage-out*", artinya input komputer akan mempengaruhi output komputer. Jika data yang diinput salah, hasilnya pasti akan salah. Pengguna (*user*) dari sistem informasi tersebut akan salah dalam melakukan pengambilan keputusan karena datanya tidak handal. Contohnya Investor salah melakukan pengambilan keputusan dalam berinvestasi karena laporan keuangan salah disajikan sehingga emiten sendiri yang dirugikan.
3. Kerugian karena penyalah-gunaan komputer
   Perusahaan yang telah menerapkan sistem informasi yang terintegrasi biasanya menyimpan data-data yang strategis (data pelanggan, data keuangan, data persediaan) di dalam komputer / *server*. Apa yang akan terjadi jika data-data tersebut disalahgunakan oleh pihak lain (*hacker, cracker*) untuk memetik keuntungan tertentu, misalnya data pelanggan, data penjualan, data yang bersifat rahasia.Berapa kerugian yang harus ditanggung oleh perusahaan?
4. Nilai dari perangkat keras, perangkat lunak, dan personil
   Investasi perangkat keras, perangkat lunak pada perusahaan yang sudah menerapkan TI, umumya relatif mahal dan bersifat jangka panjang. Di samping itu personil yang terlibat dalam aktivitas TI umumnya orang-orang yang profesional di bidangnya dan biasanya mereka meminta gaji yang memadai dengan profesinya. Apa yang terjadi jika beberapa personil tersebut meninggalkan perusahaan, pindah bekerja di perusahaan yang lain? Jika hal ini terjadi, perusahaan harus mengeluaran biaya untuk merekrut personil IT yang baru.
5. Kerugian karena kesalahan komputer
   TI sering dimanfaatkan untuk melakukan penghitungan matematis yang rumit dengan jumlah data yang besar karena kecepatan pemrosesan dan keakuratan tidak diragukan lagi. Kadang-kadang, hasil perhitungan komputer tidak seperti yang diharapkan. Contohnya sebuah bank harus menghitung bunga untuk setiap nasabah, ternyata pada bulan februari hasilnya berbeda dengan seharusnya karena setiap 4 tahun sekali, bulan februari berumur 29 hari. Kesalahan ini bisa terdeteksi setelah dilakukan audit.
6. Menjaga privasi

Data-data yang ada di perusahaan biasanya merupakan data yang rahasia misalnya data gaji, data pelanggan, data produksi, data pemasaran, atau data-data yang termasuk dalam kategori rahasia dagang (*trade secret*). Data-data tersebut tidak boleh keluar dari perusahaan karena eksistensi perusahaan bisa terganggu jika data rahasia tersebut diketahui pihak lain misalnya pesaing perusahaan sejenis.

7. Dikendalikan oleh evolusi penggunaan komputer
   Teknologi di bidang informasi dan komunikasi berkembang sangat pesat, baik dari sisi *hardware* maupun *software* termasuk *microprocessor*-nya. Teknologi yang saat ini dianggap canggih, dalam beberapa tahun akan dianggap *out-of-date*. Dampak evolusi penggunaan komputer ini berkaitan erat dengan investasi. Investasinya belum mencapai titik BEP (*Break Even Point*), telah disusul dengan perkembangan teknologi yang baru.

Teknik Audit Sistem Informasi

Teknik audit yang digunakan oleh auditor TI untuk mengaudit perusahaan yang telah menerapkan komputer dalam aktivitas bisnisnya antara lain sebagai berikut :

1. Teknik *Integrated Test Facility* (ITF)
   Pengujian ini dilakukan dengan menginput data fiktif ke dalam sistem komputer, outputnya kemudian dianalisis untuk menentukan apakah penambahan data fiktif tersebut dapat diproses secara normal oleh sistem komputer atau ada pemberitahuan (pesan) yang muncul dari sistem komputer tersebut.
2. Teknik *Embedded Audit Routine*
   Pengujian ini dilakukan dengan memasukkan sebuah program ke dalam program aplikasi yang digunakan untuk mengambil data secara berkala kemudian data yang diambil secara berkala tersebut digunakan untuk tujuan *review* dan analisis.
3. Teknik *Extended Record*
   Teknik ini mirip dengan teknik *embedded audit routine* yaitu dengan cara memodifikasi program dengan membuat data tambahan yang diambil dari aktivitas rutin. Data ini kemudian di-*review* dan dianalisis.
4. Teknik *Snapshot*
   Pengujian ini dilakukan dengan cara memodifikasi program untuk mengambil data. Data tersebut kemudian di-*review* dan dianalisis.
5. Teknik Penelusuruan
   Pengujian ini dilakukan dengan melakukan penelusuran perintah-perintah tertentu yang harus dilaksanakan sehingga bisa diketahui apakah program telah disusun secara logis atau tidak.
6. Teknik *Control Flowcharting*
   Teknik ini ditujukan untuk menguji pengendalian pada sebuah program dengan cara membuat bagan arus pengendalian pada program yang dianalisis.
7. Teknik *Mapping*
   Pengujian ini ditujukan untuk mengawasi program yang digunakan dan dari program tersebut dapat diketahui operasi apa saja yang sering dilakukan sehingga dapat dipetakan mana yang akan di-*review* lebih banyak. Biasanya teknik ini dilakukan bersamaan dengan teknik pengujian data.
8. Teknik *Review* Sistem Dokumentasi

Teknik ini ditujukan untuk me-*review* dokumentasi kegiatan di bagian IT, termasuk dokumentasi sistem dan aplikasi yang telah dibuat dan digunakan untuk pemrosesan data.

9. Pengujian dengan *Software*
   Auditor yang ingin menguji data atau *database* yang ada di *software* komputer, dapat menggunakan program khusus untuk audit dengan membuat sendiri atau menggunakan *software* yang tersedia di pasar seperti Microsoft Excel, Microsoft Acces, software ACL (*Audit Command Language*), IDEA (*Interactive Data and Extraction and Analysis*), Poc audit, dan Pan audit.

Peran Auditor

Menurut norma umum audit keempat dari norma audit satuan pengawasan intern BUMN/BUMD dinyatakan : "Auditor atau para auditor yang ditugaskan untuk melaksanakan audit, secara individu atau setidak-tidaknya secara kolektif harus mempunyai keahlian yang diperlukan dalam bidang tugasnya". Norma ini mewajibkan auditor atau para auditor dalam melaksanakan tugasnya secara individu atau secara kolektif (dalam bentuk tim) memiliki keahlian (dalam teori dan praktik). Keahlian adalah suatu kepandaian khusus yang dimiliki seseorang yang diakui mampu menggunakan teori dan praktik untuk melaksanakan profesinya. Pengertian keahlian di sini adalah baik keahlian mengenai audit maupun keahlian mengenai masalah yang diaudit. Walaupun auditor telah memenuhi keahlian yang dipersyaratkan, ia wajib meningkatkan keahliannya, termasuk di bidang teknologi informasi (TI).

Para auditor harus memahami sistem komputer karena sistem ini memiliki dampak yang besar pada operasi bisnis sebuah organisasi. Pengendalian intern pada organisasi yang berbasis komputer maupun yang belum terkomputerisasi sedikit banyak berbeda. Hal ini menimbulkan kesenjangan pada pengendalian yang mungkin akan menyebabkan timbulnya risiko-risiko baru. Jika komputer digunakan untuk memproses data akuntansi dan keuangan, auditor perlu memahami konsep dan terminologi pengolahan data dan pengendaliannya. Perlunya memahami konsep TI merupakan hal yang fundamental untuk pelaksanaan *review* yang layak dan evolusi pengolahan yang terkomputerisasi serta penggunaan komputer dalam pemeriksaan.

Perubahan lain dalam lingkungan auditor adalah kompleksitas sistem komputer. Pengembangan teknis dalam *hardware* (piranti keras) dan *software* (piranti lunak) telah meningkatkan prestasi operasi dan mengurangi biaya operasi sistem yang berbasis komputer. Akibatnya lebih banyak organisasi yang memiliki fungsi akuntansi yang diotomatisasi misalnya penyusunan daftar gaji, piutang, persediaan, dan utang. Mereka telah menerapkan sistem pengendalian manajemen yang lebih kompleks, seperti *forecasting*, perencanaan laba, dan penjadwalan produksi serta telah mengembangkan model-model perencanaan dan pengendalian aktivitas secara menyeluruh dan lebih efektif.

Menurut IAI (2001 : 335.2), kompetensi minimum yang dibutuhkan auditor dalam melaksanakan audit di lingkungan sistem informasi komputer adalah sebagai berikut :

1. Pengetahuan dasar-dasar komputer dan fungsi komputer secara umum.
2. Pengetahuan dasar tentang sistem operasi (*operating system*) dan perangkat lunak berikut :
   a. Pengetahuan signifikan dan kompleksitas operasi komputer seperti jumlah transaksi yang terjadi dan diproses.
   b. Memahami struktur organisasi dari aktivitas sistem klien dan pendistribusian proses komputer dalam entitas.

c. Pengetahuan terhadap ketersediaan data yang akan dibutuhkan oleh auditor (terkait dengan apakah sistem menyimpan dokumen, files komputer, dan buku lainnya dalam jangka waktu lama)/
d. Pengetahuan terhadap program aplikasi yang digunakan oleh perusahaan.

3. Pemahaman tentang teknik pengolahan file dan struktur data meliputi hal-hal berikut (IAI 2001 : 344.3).
   a. Pengetahuan terhadap macam-macam teknik pengolahan file. Ada berbagai teknik pengolahan file, di antaranya *On Line/Real Time Processing, On Line/Batch Processing, On Line/Memo Update* (dan pengolahan selanjutnya), *On Line / Inquiry, On Line Downloading / Uploading Processing*.
   b. Pemahaman tentang cara memasukkan informasi dalam sistem sesuai dengan jenis teknik pengolahan file apakah *On Line/Real Time Processing* atau *On Line/Batch Processing* atau teknik pengolahan file lainnya.
   c. Pengertian tentang pengolahan informasi dalam sistem.
   d. Pengetahuan mengenai waktu informasi tersebut dihasilkan dan dapat dipakai oleh *user*.
4. Berikut kemampuan bekerja dengan perangkat lunak audit
   a. Kemampuan mengoperasikan Excel sebagai salah satu CAATs termudah.
   b. Kemampuan mengoperasikan *software* audit lain, seperti ACL, IDEA.
   c. Kemampuan merancang suatu *Spesialized Audit Software* (SAS) bagi sebuah perusahaan.
   d. Penguasaan terhadap bahasa pemrograman komputer.
5. Kemampuan *me-review* sistem dokumentasi meliputi hal-hal berikut :
   a. Mampu membaca sistem dokumentasi seperti *Flowchart*, DFD, REA, ERD. *Flowchart* menggambarkan aliran dokumen yang terjadi dalam perusahaan. Data *Flow Diagram* (DFD) menggambarkan aliran data dalam perusahaan. Sementara itu, REA dan ERD menggambarkan pihak-pihak yang terkait (entitas) dalam perusahaan serta hubungan antara pihak-pihak tersebut.
   b. Mampu mengevaluasi *internal control system documentation* sehingga dapat mengidentifikasi kelemahan dan kelebihan dari kontrol yang ada.
   c. Mampu membuat / menyiapkan dokumentasi.
6. Berikut pengetahuan dasar tentang pengendalian internal Sistem Informasi Komputer (SIK) pengendalian umum dan aplikasi.
   a. Pemahaman tentang elemen dari pengendalian internal SIK beserta faktor yang ada di dalamnya.
   b. Mampu melakukan pengujian (*test of control*) terhadap semua elemen yang termasuk dalam pengendalian umum.
   c. Mampu melakukan pengujian (*test of control*) terhadap semua elemen yang termasuk dalam pengendalian aplikasi.
   d. Mampu menilai risiko pengendalian dan menerapkan *substantive test* yang sesuai dengan risiko pengendalian.
   e. Mampu memberi rekomendasi dan mendesain pengendalian umum bagi perusahaan dalam hal pengendalian umum perusahaan tersebut tidak memadai.
   f. Mampu memberi rekomendasi dan mendesain pengendalian umum bagi perusahaan dalam hal pengendalian aplikasi perusahaan tersebut tidak memadai.

7. Berikut pengetahuan memadai dalam pengembangan rencana audit dan supervisi pelaksanaan audit dalam lingkungan SIK (IAI 2001 : 335.3).
   a. Memahami dan mengetahui bagaimana fungsi Sistem Informasi Komputer diorganisasikan / bagaimana pendistribusian pengolahan komputer dalam keseluruhan entitas.
   b. Pengetahuan mengenai perangkat lunak dan keras yang digunakan oleh entitas.
   c. Pengetahuan terhadap setiap aplikasi, sifat pengolahan, dan kebijakan penyimpanan data yang diterapkan oleh perusahaan.
   d. Mampu menentukan tingkat kepercayaan yang diharapkan auditor atas pengendalian SIK.
   e. Mampu merencanakan bagaimana, dimana, dan kapan fungsi SIK akan di-*review*, termasuk penjadwalan pekerjaan tenaga ahli SIK jika digunakan.
   f. Mampu merencanakan prosedur audit yang sesuai dengan teknik audit yang akan digunakan.
8. Pemahaman dinamika perkembangan perubahan sistem dan program dalam suatu entitas.

   Kompetensi tersebut di atas akan diklasifikasikan menjadi pengetahuan dasar komputer, pemahaman mengenai teknik pengolahan file, kemampuan bekerja dengan perangkat lunak audit. Kompetensi yang akan diverifikasi dalam penelitian ini adalah kompetensi yang diperoleh dari hasil survei awal.

KESIMPULAN

Audit sistem informasi ditujukan untuk mengumpulkan dan mengevaluasi bukti-bukti untuk mengetahui apakah sebuah sistem komputer dapat melindungi aset perusahaan dan memelihara integritas data sehingga tujuan organisasi dapat dicapai secara efisien dan efektif. Para auditor dapat melakukan audit menggunakan tiga pendekatan yaitu audit di sekitar komputer, audit melalui komputer dan audit dengan komputer. Di samping itu auditor harus mempertimbangkan risiko-risiko dan pengendalian yang terkait yaitu pengendalian umum dan pengendalian aplikasi. Teknik-teknik audit yang dapat diterapkan antara lain adalah fasilitas pengujian yang terintegrasi, *embedded audit routine*, *extended record*, *snapshot*, pengendalian bagan arus, *mapping*, dan menggunakan *software* audit seperti ACL, IDEA, Microsoft Excel atau Microsoft Access. Dalam konteks ini, para auditor dituntut untuk meningkatkan kemahirannya yang terkait dengan teknologi informasi.

DAFTAR PUSTAKA

Agoes, Sukrisno dan Hoesada, Jan. 2012. *Bunga Rampai Auditing*. Jakarta : Penerbit Salemba Empat.

Akmal dan Marmah Hadi. 2010. *EDP Audit*. Jakarta : Penerbit Erlangga.

Christiawan, Yulius Jogi. 2000. Konsep Pengauditan Dalam Lingkungan Pengolahan Data Akuntansi Terkomputerisasi. *Jurnal Akuntansi & keuangan*, Vol. 2, No. 1, Mei, Hal. 9 – 20.

Fefri Indra Arza. 2007. Proses Audit pada Era Teknologi Informasi Serta Implikasi Terhadap Pembelajaran Auditing di Perguruan Tinggi. *Jurnal Akuntansi*, Vol. 2 No. 2, Desember, ISSN 1858-3687, Hal. 23-31.

Herawati, Evy. 2008. Audit Sistem Informasi Aplikasi Persediaan pada PT SS. *Commit*, Vol. 2, No. 2, Oktober, Hal. 95-98.

Julisar. 2010. Audit Sistem Informasi untuk Mewujudkan Tata Kelola Sistem Informasi (IT Governance) di Organisasi Berbasiskan Teknologi Informasi. *CSRID Journal*, Vol. 2, No.3, Oktober, Hal. 170-179.

Sasongko, Nanang. 2002. Audit Sistem Informasi : Analisis Faktor-Faktor yang Mempengaruhi Tingkat Penerapannya pada Kantor Akuntan Publik (KAP) di Indonesia. Jakarta. *Proceedings*, Komputer dan Sistem Intelijen (KOMMIT 2002)

Setiawan Herri dan Mustofa, Khabib. 2013. Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia. *Iptek-Kom*, Vol. 15, No. 1, Juni, hal. 1-15, ISSN 1410 – 3346.

Tuanakotta, Theodorus M. 2013. *Audit Berbasis ISA (International Standards on Auditing)*. Jakarta : Penerbit Salemba Empat.

Wicaksono, Aries. 2014. Audit Sistem Informasi Akuntansi Siklus Pengeluaran pada PT Lagio Furniture. *Binus Business Review*, Vol. 5, No.2, Nopember, Hal. 510 – 518.

Widayanti, Riya dan Purnamawati, Lina, 2013. Audit Sistem Informasi pada Aplikasi Sistem Manajemen Pemeriksaan (SMP) Badan Pemeriksa Keuangan Republik Indonesia. *Forum Ilmiah*, Volume 10, Nomor 2, Mei.

Widjaja Tunggal, Amin. 2001. *Audit Kecurangan (Suatu Pengantar)*. Jakarta : Harvarindo.