PENGENDALIAN PADA SISTEM INFORMASI BERBASIS KOMPUTER
(Sebuah Tantangan bagi Internal Auditor)

Ali Masjono Muchtar[1]
Ali.masjonomuchtar@akuntansi.pnj.ac.id
Ridwan Zulpi Agha[2]
Ridwan.zilfiagha@akuntansi.pnj.ac.id
[1,2] Program Studi Akuntasi, Politeknik Negeri Jakarta

ABSTRACT

Application control has changed the form of control that is usually done by humans, it now has been done by machines. The phenomenon that many types of control have been replaced by machines and has been proven by various computer applications, for example online shopping applications that have implemented comprehensive computer-based controls. Here it looks and feels real that the application control is carried out by machines, not humans. Reflecting on the analysis and implementation of controls in the Shopee online store, it can be concluded that all forms of control have been carried out by machines. The question that arises is whether the application control has prioritized humans as controllers than human control and this proven the signals proposed by (Kasali, 2017) have actually occurred. What internal auditor do in other to ensure the control exist, whether ensure the output is in accordance with computer procedures or ensure that algorithms that carry out automatic control?

Keywords; *application control, internal auditor, machine, human*

ABSTRAK

Pengendalian aplikasi telah merobah bentuk pengendalian yang biasanya dikerjakan oleh manusia telah dikerjakan oleh mesin. Fenomena bahwa banyak jenis pekerjaan yang telah digantikan oleh mesin telah dibuktikan oleh berbagai aplikasi, sebagai contoh apliksi belanja secara online yang telah menerapakan pengendalian berbasis computer secara komprehensif. Disini terlihat dan terasa nyata bahwa pengendalian aplikasi dilakukan oleh mesin, bukan manusia. Berkaca kepada analisis dan implentasi pengendalian yang ada di toko online shopee dapat disimpulkan bahwa semua bentuk pengendalian telah dikerjakan oleh mesin. Pertanyaan yang muncul adalah apakah pengendalian aplikasi tersebut telah menisbikan manusia sebagai pengendali dan sinyalemen yang dikemukan oleh (Kasali, 2017) sudah terjadi benar benar terjadi. Tantangan bagi auditor, apa yang hendak diaudit apakah memastikan outputnya sesuai dengan prosedur atau mengaudit algoritma computer yang melakukan pengendalian secara otomatis?

Kata Kunci; *pengendalian aplikasi, internal auditor, mesin, manusia*

PENDAHULUAN

Pesatnya kemajuan Teknologi Informasi dan Komunikasi (TIK) pada era sekarang telah membawa berbagai konsekwensi posistip dan konsekwensi negatip dalam bidang pengendalian. Banyak jenis pekerjaan yang telah digantikan oleh robot (Kasali, 2017). Salah satu pekerjaan yang akan berkurang adalah pekerjaan akuntan, dalam tulisan ini identik dengan auditor. Banyak juga manfaat yang didapat dari kemajuan tersebut diantaranya dapat menggantikan pekerjaan manusia yang berulang-ulang dan membosankan.

Salah satu pekerjaan akuntan adalah mengaudit berbagai bentuk pengendalian yang ada di suatu sistem atau yang ada di suatu entitas untuk memastikan bahwa pengendalian dimaksud ada dan berfungsi dengan baik. Jika berfungsi dengan baik maka pengendalian tersebut sudah dapat menjaga aset organisasi dan organisasi beroperasi dengan efektif dan efisien.

Hampir setiap kegiatan manusia telah digantikan oleh aplikasi, banyak sekali contoh aplikasi yang saat ini digunakan oleh manusia untuk menggantikan pekerjaan yang biasanya dikerjakan oleh manusia. Aplikasi yang digunakan oleh manusia didalamnya dapat dipastikan ada pengendalian, ada dua jenis pengendalian yaitu pengendalian umum dan pengendalian aplikasi (Romney & Steinbart, 2017). (Weber, 1999).

Fokus tulisan ini adalah pengendalian aplikasi yang dapat dipastikan ada disetiap aplikasi apapun yang menggunakan TIK. Dilihat dari siklus akuntansi, maka disetiap siklus tersebut dipastikan ada pengendalian karena disetiap siklus ada potensi ancaman, potensi ketidakteraturan, potensi penyalahgunaan wewenang dan potensi kecurangan yang dapat terjadi sewaktu waktu.

Permasalahan

Permasalah utama yang hendak dikaji dalam tulisan ini adalah pengendalian yang ada di berbagai aplikasi telah menggantikan peran manusia, hal ini mendukung sinyalemen yang diberikan oleh Kasali (2017). Apakah pengendalian yang ada di aplikasi tersebut menisbikan peran manusia sehingga peran manusia lebih sedikit atau hilang sama sekali. Manusia hanya memastikan perangkat keras dan perangkat lunak beroperasi secara teratur dan peran inipun sudah dapat digantikan oleh robot robot canggih lainnya. Tidak diperlukan lagi keterlibatan manusia dalam memastikan bahwa saldo kas cukup, bahwa semua otoritisasi berfungsi dengan baik, bahwa semua yang melakukan aktivitas terdeteksi dengan baik, jelas dan terukur. Peran internal auditor mungkin akan bergeser, tidak lagi memastikan bahwa pengendalian ada tetapi memastikan bahwa output dari aplikasi tersebut telah sesuai dengan kriteria "reliability".

Tujuan

Tujuan dari penulisan artikel ini adalah mendeskripsi dan mengidentifikasi fungsi fungsi kontrol yang ada di aplikasi dan seberapa besar fungsi tersebut teleh dilakukan oleh robot. Menganalisis apakah fungsi kontrol tersebut dapat menggantikan peran manusia untuk memastikan bahwa pengendalian terhadap aplikasi benar benar dapat digantikan oleh mesin.

TINJAUAN PUSTAKA

Kontrol aplikasi adalah salah satu strategi mitigasi paling efektif dalam memastikan keamanan sistem. Pengendalian aplikasi adalah pendekatan keamanan untuk memprotek sistem dari kode-kode jahat (*malicious*) yang dijalankan di dalamnya. Ketika pengamanan sistem sangat kuat maka dapat diyakini bahwa hanya aplikasi dan pengguna yang sah dan di otorisan yang dapat mengekesekusi aplikasi tersebut. (ACSC, 2021)

Disisi lain, pengedalian pada sistem informasi terbagi atas pengendalian umum atau *(general control*) dan pengendalian aplikasi. Pusat pengendalian ada pada pengendalian aplikasi karena pengendalian aplikasi sangat dekat dengan data dan semua user, termasuk pelanggan menggunakan aplikasi. (Weber, 1999)

Pengendalian aplikasi adalah praktek mengamankan sistem dengan membatasi pengguna yang tidak berhak untuk dapat melakukan berbagai tindakan di dalam aplikasi, termasuk didalamnya *Validity checks, Identification, authentication, authorization, input control, forensic control* dan lainnya. (Lord, 2001)

Pengendalian aplikasi ditujukan untuk meyakinkan bahwa setiap sistem aplikasi yang digunakan oleh suatu organisasi dapat menjaga asset, memaintain integritas data dan dapat mencapai tujuan secara efisien dan efektif. (Weber, 1999).

Secara umum pengendalian dalam system informasi terbagi menjadi dua katagori besar yaitu pengendalian umum dan pengendalian aplikasi (Romney & Steinbart, 2017). (Weber, 1999). Pengendalian umum lebih difokuskan kepada masalah tatakelola sistem teknologi yang digunakan oleh suatu orgnisasi. Pengendalian umum mulai dari *Top Managemen Control, Information System Management Control, System Development Control, programming Control, Data Administration Control, Qualtiy assurance Control, Security Administration Control, Operation Controls*. (Weber, 1999). Pengendalian umum untuk memastikan bahwa tatakelola sistem informasi organisasi sesuai dengan standar yang telah ditetapkan perusahaan dan dapat menjaga aset perusahaan serta operasional perusahaan beroperasi secara efisien dan efektif.

Pengendalian aplikasi terdiri dari *Boundary control, Input Control, Communication Control, Process Control, Database Control, Ouput Control*. (Weber, 1999). Pengendalian aplikasi melekat disetiap aplikasi yang digunakan oleh pengguna. Jadi setiap aplikasi yang di duplikat, pengendalian aplikasi selalu ada dan dipastikan berfungsi dengan baik. Lain halnya dengan pengendalian umum yang tidak melekat di aplikasi namun melekat pada sistem tatakelola sistem informasi yang kendalikan mulai dari *top management* sampai ke *operational management.*

Pengendalian aplikasi menjadi sentral dari semua bentuk pengendalian karena aplikasi digunakan oleh semua pegawai di suatu organisasi, bahkan organisasi rela dan menyarankan pelanggan mereka untuk menggunakan aplikasi. Dengan demikian aplikasi yang dapat digunakan oleh semua orang, baik internal maupun ekternal organisasi haruslah memiliki pengendalian yang dapat dipercaya (*reliability*) dan aplikasi tersebut diyakini dapat menjaga aset perusahaan.

Boundary control merupakan kompoenen antarmuka antara pengguna dan sistem. Guna pengendalian ini antara lain memastikan bahwa identitas dan otentias dari pengguna sistem adalah valid, memastikan bahwa identitas yang digunakan berhak untuk menggunakan sumber daya yang ada di sistem komputer dan membatasi tidakan apa yang bisa dilakukan oleh user yang menggunakan identitas tersebut. (Weber, 1999)

Pengendalian ini terpusat kepada bagaimana akses ke dalam suatu sistem. Situasi terkini *boundary control* tersebut sudah dapat dilakukan oleh sistem, artinya semua bentuk pengendalian telah dikendalikan oleh algoritma yang ketat dan pengguna wajib mematuhinya. Sebagai contoh penggunaan kombinasi password yang rumit, penggunaan enkripsi, penggunaan One Time Password (OTP), proses otentikasi dan konfirmasi ke media lain yang dapat mengendalikan akses ke sebuah sistem atau aplikasi.

Sejalan dengan *boundary control* adalah *input control* yang mengendalikan bagaimana data diinput ke aplikasi, menyiapkan berbagai cara agar data yang di input 100% akurat, tidak ada kesalahan. Dalam penerapannya, pengendalian input sudah dikendalikan oleh sistem, misalnya penggunaan barcode, penggunaan scanner, untuk memastikan akurasi input.

Communication control terdiri dari komponen yang bertanggung jawab memindahkan (trasmit) dari dari satu sistem ke sistem lain, misalnya mengendalikan perpindahan data dari *flasdisk* ke *printer*, dari satu komputer ke komputer lain. Semua bentuk pengendalian sudah menggunakan sistem, campur tangan manusia sangat minim, bahkan tidak ada.

Process control memastikan proses yang terjadi di dalam sistem, antara lain komputasi, cklasifikasi, mengurut data, dan membuat ringkasan sudah sesuai dengan ketentuan yang ada di sistem atau di aplikasi tersebut. Semua bentuk pengendalian proses ini menggunakan algoritma yang telah dibuat oleh programmer. Pengguna hanya memastikan bahwa pengendalian tersebut benar benar telah beroperasi dengan baik.

Database control adalah komponen yang bertanggung jawab mendesain kerangkan database, mendefenisikan fungsi penambahan data, memodifikasi data. Dalam penerappannya ad dua kontrol yaiitu *database control* dan *data control*. Keduanya mengendalikan database. Jika *data control* lebih fokus kepada mengendalikan siapa dan aplikasi apa yang boleh akses ke database sesuai dengan batasan batasan yang ada. Sedangkan *database control* lebih fokus kepada bagaimana data tersebut dapat menghasilkan output yang sesuai dengan keiinginan pengguna.

Output control adalah komponen yang mengendalikan mengambil (retrieve) data dan mempresentasikannya untuk pengguna. Otomatisasi sistem ouput dari sebuah aplikasi memberikan kemudahan pendistribusian dan menyebar informasi hanya kepada orang orang yang berhak, terhidar dari upaya modifikasi. Dalam penerapannya penggunaan output dalam bentuk pdf sudah banyak digunakan oleh berbagai aplikasi. File dalam bentuk pdf sudah menjadi standar output dan perubahan yang terjadi di file tersebut akan mudah terdeteksi.

Apakah sistem pengendalian dapat mengidentifikasi aplikasi/user yang disetujui. Mengembangkan aturan kontrol aplikasi untuk memastikan hanya aplikasi yang disetujui yang diizinkan untuk dijalankan. memelihara aturan kontrol aplikasi menggunakan program manajemen perubahan. memvalidasi aturan kontrol aplikasi secara tahunan atau lebih sering.

Saat menentukan bagaimana menerapkan kontrol aplikasi, metode berikut

dianggap cocok jika diterapkan aturan penggunaan kriptografis, aturan penerbitan sertifikat (menggabungkan nama penerbit dan nama produk), aturan jalur (memastikan izin sistem file dikonfigurasi untuk mencegah modifikasi folder dan file yang tidak sah izin, isi folder dan file individual). (ACSC, 2021)

METODOLOGI

Penulisan artikel ini menggunakan metode kualitatif. Data yang digunakan dari berbagai sumber yang valid dalam arti sesuai dengan kaidah sebuah sumber yang dapat dipertanggungjawabkan dan dapat ditelusuri secara online. Pembahasan menekankan kepada aspek penggunaan teknologi informasi dalam berbagai aplikasi dan pengendalian aplikasi.

HASIL DAN PEMBAHASAN

Fungsi pengendalian yang sudah di jelaskan di sub bab sebelumnya telah diimpelementasikan pada berbagai aplikasi yang merupakan fungsi kontrol yang ada di siklus akuntansi. Contoh nyata yang paling banyak dirasakan oleh pengguna aplikasi adalah adanya sistem konfirmasi menggunakan media lain, misalnya konfirmasi perubahan password akan di lakukan dengan menggunakan email atau no HP, dengan demikian dapat dipercaya bahwa pengguna yang mengganti password adalah orang tepat. Semua proses ini dilakukan oleh sistem, peran kita sebagai manusia hanya sebagai pengguna dan semua prosedur telah ditentukan oleh sistem, pengguna tidak dapat menghidari.

Untuk memastikan pesanan dilakukan oleh pelanggan yang terdaftar maka setiap pesanan selalu disyaratkan adanya *login ID* dan *Password.* Untuk memastikan bahwa pesanan barang yang dibeli selalu digunakan kode barang yang diwakili oleh gambar, sehingga pelanggan tidak mengetikan kode barang tetapi mengklik gambar.

Untuk memastikan bahwa pesanan tersebut telah dibayar ada prosedur yang menghubungkan pelanggan, bank dan toko, sehingga ketiganya memiliki fungsi pengendalian masing masing.

Di siklus akuntansi ada beberapa hal yang selalu terjadi kesalahan jika dilakukan secara manual. Misalnya tidak akuratnya data induk atau ada perbedaan antara data induk dengan data yang yang digunakan oleh aplikasi. Untuk mengatasi hal ini aplikasi memiliki pengendalian yang disebut *data processing integrity* yang memastikan adanya kaitan atau *relationship* antara data induk dan data di aplikasi. Di tempat penyimpanan data (data induk) ada proses yang membatasi aplikasi atau pengguna untuk bisa akses dan ada prosedur mereview setiap perubahan di data induk dan diterapakan metode enkripsi. Ada sistem enkripsi yang membatasi pengguna untuk melihat data di tempat penyimpanan data. Kesemuanya ini dilakukan oleh aplikasi yang menggunakan algoritma yang ketat dan wajib dipatuhi oleh pengguna, jika tidak dipatuhi maka proses akan tertunda atau digantung (*hang*) sampai pengguna mengambil tindakan.

Untuk menghidari kehilangan data, diperlukan *back-up data* secara *reguler*, banyak sistem *backup-data* yang ditawarkan oleh pihak ketiga, adanya aplikasi yang dapat membackup data secara langsung, setiap menit, dan backup secara harian, mingguan dan bulanan. Semua dilakukan demi terjaminnya database tidak hilang dan terkendali dengan baik. Dengan adanya sysstem cloud, backup data akan dapat dilakukan secara terus menerus dan ada jaminan bahwa data tersebut tidak akan hilang.

Untuk menghidari ketidaksesuaian data yang diinput (*inacccurate data entry*), aplikasi memiliki fungsi *data aentry control* misalnya *validity checks, identification, authentication, authorization, input controls, and forensic controls* (Lord, 2001) yang telah diotomatisasi sehingga pengguna terpaksa atau dipaksa untuk patuh.

Kesalahan yang sering terjadi adalah adanya pengungkapan informasi sensitif yang tidak sah sehingga pengguna yang tidak berhak dapat melihat informasi tersebut. Aplikasi telah didesain sedemikian rupa agar hanya informasi tertentu yang dapat dipublikasikan, disinilah peran *authorization* dan *authentication* dioperasikan dengan ketat saat login.

Uncollectible accounts menjadi masalah tersendiri terutama untuk penjualan kredit. sistem telah didesain untuk menghendle apakah ada *account* yang melebihi kredit limit, apakah ada *account* yang menunggak melewati batas waktu. Untuk mengatasi hal ini aplikasi telah didesain memiliki mekanisme untuk *approve* setiap ada perubahan kebijakan. Misalnya oprator hanya diberihak untuk melakukan penjualan kredit sesuai dengan limit yang tertera di aplikasi dan tidak berhak untuk melakukan perubahan. Untuk melakukan perubahan harus ada *arppove* dari atas langsung

yang dilakukan secara tersistem dimana atasan langsung wajib memberikan *approval* dengan memasukan PIN atau password persetujuan.

Komunikasi antara pengguna dengan tempat penyimpanan data sangat vital karena aplikasi ada di computer atau HP pengguna sedangkan data ada di tempat penyimpanan data perusahaan. Komuniasi kedua entitas ini harus dikendalikan dengan kuat karena jalur inilah tempat para *hacker* untuk bisa masuk ke sumber data perusahaan (*piggybacking*). Ada sistem *enkiripsi end to end* akan memprotek data dan informasi yang lewat di saluran komunikasi. secara umum dapat dikatakan jalur komunisasi yang digunakna oleh perusahaan sudah mengantisipasi hal ini dengan berbagai software dan mekanisme authentikasi yang otomatis.

Database sebagai tempat penyimpanan data, merupakan asset perusahaan yang wajib dijaga selama 24 jam. Peran Database administrator dan data administrator sangat dominan dalam memodifikasi database dan mengendalikan akses ke database. Database administrator cenderung kepada peran sebagai pengaturan struktur dan desain tabel tempat penyimpanan data, sedangkan data administrator lebih cenderung kepada pengaturan penggunaan. Mengatur hak akses pengguna dan hal akses aplikasi yang sesuai dengan kebijakan perusahaa. Ditempat penyimpanan data juga berlakuk system enkripsi untuk memastikan hanya pengguna/aplikasi yang diberi hal saja yang dapat membaca dan mengakses data tersebut.

Disamping itu pengendalian di database juga mengatur pengaturan hak pengguna atau aplikasi, ada yang diberikan *modify* yang dapat melakukan membaca, menyimpan dan merobah data, ada hak *read* dimana pengguna hanya bisa membaca data dan hak membaca *aggregate data* (*statistical data*), dan ada hak *add* yang berhak untuk melakukan append (membaca data) dan *insert* (menyisip data).

Kunci utama dari pengendalian pada sistem berbasis computer ada pada *integritas*, baik integritas data yang mampu mengsikronkan data yang digunakan oleh berbagai aplikasi atau pengguna secara bersamaan dari berbagai tempat. *Interiritas* lainnya yang mampu mengsingkronkan *authentication* dan *authorization* dietiap kali aplikasi digunkan.

Pengendalian aplikasi berbeda dengan pengendalian manajemen dalam beberapa hal berikut ini. Pengendalian aplikasi melibatkan hardware dan software bukan SDM. Pengendalian aplikasi diterapkan pada data dan prosesnya, bukan pada proses pengembangan, maintenan dan proses operasional sistem. Pengendalian aplikasi ada pada setiap sistem aplikasi dan berhubungan dengan biaya dan manfaat. Sedangkan pengendalian manajemen bergantung kepada analisis biaya dan manfaat terhadap aplikasi secara menyeluruh.

Pengendalian aplikasi cenderung fokus kepada penjagaan asset (penjagaan terhadap kemungkinan hilang, pemindahan, penghancuran) dan memaintain integritas data (meyakinkan otorisasi penggunaan, lengkap, akurat dan tidak terjadi pengulangan penyimpanan data). (ACSC, 2021), (Lord, 2001), (Weber, 1999).

Semua bentuk pengendalian aplikasi yang telah dijelaskan diatas telah diimplementasikan pada berbagai aplikasi, sebagai contohnya dan dapat dirasakan oleh pelanggan toko online, misalnya pelanggan Shopee. Mulai dari registrasi sampai kepada barang sampai kerumah dikendaliakan oleh sistem, sehingga timbul pertnayaan siapa yang mengerjakan semua bentuk pengendalian tersebut.

Disini terlihat dan terasa nyata bahwa pengendalian aplikasi dilakukan oleh mesin, bukan manusia. Berkaca kepada analisis dan implentasi pengendalian yang ada di toko *online shopee* dapat disimpulkan bahwa semua bentuk pengendalian telah dikerjakan oleh mesin. Pertanyaan yang muncul adalah apakah pengendalian aplikasi tersebut telah menisbikan manusia sebagai pengendali dan sinyalemen yang dikemukan oleh (Kasali, 2017) sudah terjadi benar benar terjadi.

KESIMPULAN

Pengendalian aplikasi melibatkan hardware dan software bukan manusia. Berbagai fungsi pengendalian yang telah diterapkan pada semua aplikasi dapat menjaga aset perusahaan, mulai dari *boundary countrol, input control, process control, database control, communcation control*, sampai kepada *output control*. Peran manusia sangat minim, manusia hanya sebagai pengguna aplikasi.

REFERENCES

ACSC, A. C. (2021, Oct). *Australian Cyber Security Centre*. Retrieved from Implementing Application Control: https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control

Kasali, R. (2017, Oct 18). *Inilah Pekerjaan Yang akan Hilang Akibat "Disruption"*. Retrieved Feb Tuesday, 2022, from Rumah perubahan: https://www.rumahperubahan.co.id/blog/2017/10/18/inilah-pekerjaan-yang-akan-hilang-akibat-disruption/

Lord, N. (2001, December Tuesday). *What is Application Control? Definition, Best Practices & More.* Retrieved from Digital Guardian: https://digitalguardian.com/blog/what-application-control

Romney, M. B., & Steinbart, P. J. (2017). *Accounting Information System.* Pearson.

Weber, R. (1999). *Infomation Systems Control and Audit.* New Jearsy: Premtice Hall.