

AUDIT SISTEM APLIKASI

Sasaran :

1. Memahami pedoman umum audit untuk sistem aplikasi
2. Memahami kebijaksanaan umum dalam pelaksanaan audit untuk sistem aplikasi
3. Memahami pendekatan audit pada struktur kontrol internal

PEDOMAN UMUM

Sejumlah pedoman umum dapat digunakan dalam proses audit pada sistem aplikasi, di antaranya adalah:

1. Terdapat jejak audit (*audit trail*) yang jelas sehingga semua transaksi yang di-*input*-kan ke dalam sistem dapat ditelusuri melalui *output file* dan *print out* laporan-laporan yang dihasilkan oleh sistem tersebut.

Contoh: Input transaksi yang dilakukan *teller* tabungan dapat diperiksa kembali kebenarannya melalui Daftar Mutasi Harian atau diperiksa pada *file* yang terpengaruh akibat transaksi tersebut, misalnya *file* Grtran.dbf.

2. Dokumen-dokumen sumber atau *format* pemasukan data pada layar harus dibuat sedemikian rupa sehingga dapat meminimalkan kesalahan-kesalahan maupun kelalaian yang sering dilakukan oleh manusia (*human error*).

Contoh:

- *Check digit* yang ada pada struktur nomor rekening nasabah sangat berguna untuk mengantisipasi kesalahan pemasukan nomor rekening oleh *teller*. Jika *teller* melakukan kesalahan dalam

pemasukan nomor rekening tersebut, sistem akan memberikan pesan kesalahan sehingga *teller* yang bersangkutan segera menyadari kekeliruannya.

- *Length of field* dari tampilan *input* sudah ditentukan terlebih dahulu pada saat perancangan struktur *database*, misalnya untuk *input* nilai nominal transaksi.

3. Input transaksi harus secara teliti diperiksa dan divalidasi sehingga data yang di-*input*-kan sesuai dengan yang tertulis pada dokumen, *slip*, formulir atau *form-form* lain.

Contoh: Data transaksi yang terdapat pada Daftar Mutasi Harian dicocokkan dengan masing-masing *slip* transaksi.

4. Aplikasi yang digunakan harus dapat memberikan informasi mengenai sistem keamanan yang ada atau dapat menunjukkan suatu mekanisme yang dapat meyakinkan auditor bahwa hanya pejabat yang berwenang yang dapat mengakses aplikasi tersebut.

Contoh: Seorang *teller* dengan *User-ID* K04 berwenang untuk mengakses menu *teller*, yaitu fasilitas pemasukan transaksi pada Aplikasi Tabungan. *Teller* tersebut tidak berhak mengakses menu *Head Teller*, namun apabila ia mencoba untuk mengakses menu tersebut maka sistem akan memberikan pesan berikut:

“Anda tidak berwenang menggunakannya!”

5. Jika memungkinkan, prosedur *batch control* dapat digunakan pada aplikasi untuk meyakinkan bahwa semua sudah benar dan lengkap.
6. Prosedur penanganan untuk kesalahan yang terjadi pada suatu transaksi harus ada dan dapat ditelusuri melalui laporan kesalahan yang dihasilkan. Oleh karena itu, diperlukan adanya bagan alir

(*flowchart*) sistem dan prosedur dari setiap kegiatan yang ada pada sistem aplikasi.

Kontrol transaksi pada sistem aplikasi, menurut Jenkins dkk., (19??), mempunyai 3 sasaran, yaitu:

1. *Completeness*, untuk meyakinkan bahwa seluruh transaksi sudah di-*input*-kan secara lengkap dan seluruhnya sudah tersimpan dalam sistem, serta telah diproses melalui suatu sistem akuntansi;
2. *Accuracy*, untuk meyakinkan bahwa semua transaksi telah disimpan dengan benar/akurat, telah dimasukkan ke dalam sistem dan telah diproses melalui suatu sistem akuntansi; dan
3. *Authorisation*, untuk meyakinkan bahwa hanya transaksi yang benar yang diproses.

Penggunaan sarana TSI di samping menunjang operasional bank, juga mengandung risiko yang dapat mengakibatkan kerugian, baik yang bersifat finansial maupun non-finansial. Oleh karena itu peranan dan fungsi pengendalian internal TSI menjadi semakin penting dan perlu dilakukan oleh manajemen bank sebagai salah satu upaya meminimalkan kerugian dimaksud. Pengendalian internal TSI tersebut terutama bertujuan untuk menjamin integritas data serta kelangsungan operasional bank (Bank Indonesia, 1995). Pengendalian internal TSI antara lain meliputi:

- Data bank telah diproses secara lengkap, aman, tepat waktu dan benar;
- Informasi keuangan dapat diandalkan;
- Prosedur operasi TSI dilaksanakan secara efektif dan efisien;
- Kelangsungan operasi TSI dan kegiatan operasional bank; dan
- Kepatuhan terhadap ketentuan yang berlaku.

Keberhasilan fungsi audit TSI dalam mencapai tujuan sebagaimana dikemukakan di atas sangat tergantung dari kebebasan (*independensi*) auditor internal TSI dalam melaksanakan tugasnya. Hal ini akan tercermin

dari kedudukan satuan kerja tersebut dalam struktur organisasi bank, sistem pelaporan serta tanggung jawab yang diberikan manajemen.

KEBIJAKSANAAN UMUM AUDIT

Bank perlu memiliki pedoman audit TSI tertulis dan disetujui oleh manajemen. Pedoman tersebut di samping digunakan sebagai sarana untuk mencapai hasil audit yang efektif dan efisien, juga merupakan pedoman bagi manajemen dalam menilai kinerja fungsi audit internal TSI. Pedoman tersebut perlu memuat petunjuk mengenai hal-hal berikut:

- Struktur organisasi dan sistem pelaporan;
- Penentuan frekuensi dan jadwal audit;
- Keterlibatan satuan kerja audit internal TSI pada pengembangan sistem;
- Prosedur audit internal TSI;
- Standar kertas kerja, isi dan format laporan hasil audit, dokumentasi dan distribusi serta pemantauan tindak lanjutnya; dan
- Standar dan prosedur pengembangan, dokumentasi, pemeliharaan serta pengawasan terhadap penggunaan perangkat lunak audit.

PENDEKATAN AUDIT PADA STRUKTUR *INTERNAL CONTROL*

Beberapa elemen struktur kontrol internal (*internal control*) dalam pendekatan audit terbagi ke dalam beberapa hal, diantaranya adalah:

- ***Control Environment***

Control environment meliputi *attitudes, abilities, perception, dan actions* dari para anggota organisasi, terutama dari pihak manajemen.

Beberapa faktor dari *control environment* tersebut meliputi:

1. Peraturan dari *board of directors* dan komite audit dalam menerapkan prinsip-prinsip akuntansi dan memprediksikan perkembangan di masa yang akan datang;

2. Ruang lingkup perkembangan kegiatan bisnis yang dapat menyebabkan adanya kesalahan ketertinggalan sistem aplikasi yang digunakan;
3. Kecukupan perolehan informasi yang digunakan dalam membuat keputusan dan estimasi pengembangan di masa yang akan datang; dan
4. Kompetensi dari para petugas yang memiliki tanggung jawab dalam pengembangan sistem aplikasi.

- **Accounting System**

Pada dekade sekarang ini hampir seluruh sistem akuntansi sudah dilakukan dengan komputer, sehingga selalu dilengkapi dengan prosedur manual dan prosedur sistem aplikasi komputer sebagai dasar untuk melakukan *input* data, *processing*, dan *maintenance* (pemeliharaannya).

- **Control Procedures**

Control procedures pada sistem aplikasi dapat dilakukan baik dari sistem aplikasi itu sendiri (otomatik) maupun secara manual, tetapi umumnya *control procedures* dilakukan melalui kedua metode tersebut. Kegiatan ini meliputi kontrol dan monitoring terhadap kegiatan-kegiatan yang berhubungan dengan pemrosesan data yang tidak dapat berfungsi dengan baik. Sebagai contoh, apabila prosedur dalam sistem aplikasi komputer tidak berjalan dengan semestinya yang tercermin pada *report output* sistem tersebut, maka auditor harus melakukan pelacakan baik secara manual maupun secara sistem terhadap kesalahan tersebut.

- **Control Risk**

Control risk didefinisikan sebagai kontrol terhadap risiko yang muncul karena adanya kesalahan yang signifikan atau kesalahan material. Hal ini dapat terjadi karena adanya suatu risiko yang masih belum

terdeteksi dan ter-cover upaya penanggulangannya pada kegiatan kontrol internal.

AUDIT KEAMANAN SISTEM

Sistem aplikasi yang dimiliki suatu organisasi haruslah mencakup tiga hal pokok yang dapat dijadikan acuan dalam kerangka audit, *control* dan *security*. Ketiga hal tersebut adalah:

- **Integritas (*Integrity*)**

Sistem aplikasi yang digunakan haruslah selalu mengembangkan sistem yang mempunyai integritas fungsional, yaitu kemampuan untuk melanjutkan operasi, walaupun salah satu atau lebih dari komponennya tidak berjalan dengan baik.

- **Audibilitas (*audibility*)**

Apabila sebuah sistem memiliki auditabilitas, maka akan mudah bagi auditor untuk melakukan pemeriksaan, verifikasi atau bahkan melakukan demonstrasi tampilannya. Terhadap sistem aplikasi yang digunakan tersebut haruslah dilakukan pengujian *accountability* (kemampuan penghitungan) dan *visibility* (visibilitas) agar dapat disebut sebagai sistem yang audibel.

Accountability berarti bahwa setiap adanya suatu perubahan dalam sistem dapat dilakukan pelacakan prosedur pertanggung jawabannya (*audit trail*). Sedangkan *visibility* (visibilitas) berarti bahwa adanya kesalahan dalam penampilan sistem tersebut dapat segera diketahui oleh manajer sistem.

- **Berdaya kontrol**

Manajemen sebuah organisasi dapat melakukan pengerahan dan penghambatan pengaruh apabila sistem aplikasi tersebut memiliki daya kontrol. Teknik yang efektif dalam menerapkan daya kontrol sistem ini

adalah dengan membagi sistem menjadi beberapa subsistem yang menangani transaksi secara terpisah. Kegagalan keamanan pada satu subsistem tidak akan berpengaruh pada keseluruhan sistem.

AUDIT KONTROL MANAJEMEN

Sejumlah mekanisme kontrol sistem aplikasi dapat dijadikan sebagai pedoman umum bagi pihak manajemen dalam sebuah organisasi. Di antaranya adalah:

- **Pertama**, manajemen dapat melakukan kontrol langsung, yaitu melakukan evaluasi kemajuan dan penampilan dari suatu sistem aplikasi, serta menentukan tindakan koreksi (apabila diperlukan) yang harus dilakukan;
- **Kedua**, manajemen melakukan kontrol secara *continue* (terus menerus) melalui petugas yang bertanggungjawab terhadap sistem aplikasi, sehingga kegiatan operasi sistem aplikasi yang digunakan selalu *up to date* dan terjaga kelangsungannya; dan
- **Ketiga**, manajemen melakukan kontrol terhadap sistem aplikasi secara tidak langsung dengan melalui auditor internal atau eksternal, sehingga diharapkan mekanisme kontrol terhadap sistem aplikasi akan langsung ditangani oleh spesialis.

TEKNIK AUDIT SISTEM APLIKASI

Pedoman ini diperlukan untuk melakukan audit terhadap manajemen TSI, sistem dan pemrograman, operasi komputer dan pengamanan fisik, integritas data dan aplikasi, serta efektivitas penyelenggara kontrol dan pengamanan informasi pada satuan kerja pengguna. Pedoman audit TSI agar selalu disesuaikan secara berkala dan terhadap perubahan yang dilakukan, perlu mendapat persetujuan dari manajemen bank.

Pelaksanaan audit internal TSI sangat tergantung pada kompleksitas sistem TSI serta kemampuan pemeriksa. Agar pelaksanaan audit TSI

dapat terlaksana secara efektif maka auditor intern TSI perlu memiliki (Bank Indonesia, 1995) kualifikasi berikut:

Pengetahuan dasar:

- Akuntansi dan Prinsip-prinsip Akuntansi Perbankan Indonesia;
- Konsep manajemen dan pelaksanaannya serta prinsip-prinsip dasar audit internal;
- Konsep dan Teknik audit TSI;
- Teknologi dan analisis risiko;
- Desain dan tahapan pengembangan sistem; dan
- Sistem operasi, aplikasi, sistem pengelolaan data dan kontrol TSI.

Kemampuan yang memadai untuk:

- Melaksanakan audit dan mendokumentasikan kertas kerja audit;
- Berkomunikasi secara efektif; dan
- Melaporkan hasil temuan audit;

Dalam audit internal TSI beberapa hal yang perlu untuk mendapatkan perhatian dari pemeriksa, di antaranya, adalah (Bank Indonesia, 1995):

- Menilai kepatuhan terhadap ketentuan yang berlaku, kebijaksanaan, rencana dan prosedur yang telah ditegaskan;
- Menilai kebenaran penerapan prinsip-prinsip akuntansi Aplikasi Keuangan yang dilaksanakan serta kecukupan kontrol pengoperasiannya;
- Memastikan pengamanan asset bank terhadap risiko digunakannya TSI;
- Memastikan bahwa data bank telah diproses secara lengkap, akurat, dan tepat waktu; dan
- Menyarankan alternatif perbaikan untuk mengatasi kekurangan di bidang kontrol.

Evaluasi Posisi/Description – Non Officer		
Permanen		Perubahan Sementara
Posisi:	Junior clerk	<i>Job grade</i> sekarang:
Departemen:	DPC	Nama petugas: Edi
Dibuat oleh:	Heru	Diusulkan <i>job grade</i> :
Disetujui oleh:		Disetujui oleh:
Tugas Pokok:		
<ol style="list-style-type: none"> 1. <i>Backup server & cartridge</i>; 2. Proses Akhir Hari; 3. Proses akhir bulan; 4. Buka/tutup sistem tabungan, giro, dan deposito; 5. Monitor <i>on line</i>; dan 6. Install aplikasi baru dari kantor pusat. 		
Tanggung jawab utama/tugas		
<ol style="list-style-type: none"> 1. <i>Backup server</i> untuk menghindari risiko akibat kerusakan <i>main server</i>; 2. Proses akhir hari, cek saldo, otorisasi, <i>posting GL</i>, <i>print</i> daftar OD, daftar saldo, <i>refer item</i>; 3. 		

Gambar 4.1 Contoh Kartu Evaluasi Posisi

Hal-hal yang perlu diperiksa dalam Aplikasi Perbankan adalah sebagai berikut:

Tabel 4.1 Butir-butir Pemeriksaan dalam Aplikasi Perbankan

No.	Keterangan
1.	<i>Check list</i> (harian/bulanan/tahunan)
2.	<i>Call back</i>
3.	Saldo individu dicocokkan dengan <i>General Ledger</i> ;
4.	Laporan selisih <i>offset</i> harus 0 (nol);
5.	Daftar mutasi yang dihapus;
6.	Daftar mutasi <i>back value</i> ;
7.	Daftar <i>stop payment order</i> ;
8.	Batasan wewenang <i>teller</i> ;
9.	Batasan wewenang fungsi program;
10.	Staff <i>ID</i> yang cuti
11.	Daftar <i>alternate</i> ;
12.	Peng-input-an data/konversi
13.	Perubahan data nasabah.

Dalam Gambar 4.2 dan 4.3 disajikan contoh-contoh checklist, berturut-turut, dalam Aplikasi Tabungan dan Aplikasi Giro.

No.	Kegiatan	User ID	Jam	Paraf
Awal hari				
1.	Buka sistem			
Akhir hari				
1.	<i>Back up</i> data sebelum proses akhir			
2.	Cetak laporan yang diperlukan			
3.	Membuat transaksi <i>General Ledger (GL)</i>			
4.	Cetak mutasi per nota			
5.	<i>Posting</i> transaksi tabungan ke <i>GL</i>			
6.	Proses akhir hari			
7.	<i>Back up</i> data setelah proses akhir			
8.	Tutup sistem			
Akhir bulan				
1.	Cetak biaya administrasi			
2.	Perhitungan akhir bulan			
3.	Backup data setelah perhit. Akh-bul			
4.	Cetak laporan yang diperlukan (daftar biaya meterai dicetak pada akhir tahun)			
5.	Proses akhir bulan			
6.	Backup data setelah proses akh-bul			
7.	Tutup sistem			
Catatan: Khusus akhir bulan, menu <u>akhir hari</u> nomor 5 di atas baru dilakukan setelah akhir bulan nomor 2 telah dilakukan.				

Gambar 4.2 Contoh *Checklist* dalam Aplikasi Tabungan

No.	Kegiatan	User ID	Jam	Paraf
Awal hari				
1.	Buka sistem			
Akhir hari				
1.	Cetak laporan yang diperlukan			
2.	Cek & penyesuaian saldo			
3.	Otorisasi seluruh departemen			
4.	Membuat transaksi <i>GL</i>			
5.	Cetak mutasi per nota			
6.	Posting transaksi giro ke <i>GL</i> (setelah biaya kliring di giro dicetak dan di- <i>posting</i>)			
7.	Cek saldo subbuku besar giro dengan <i>GL</i>			
8.	<i>Back up</i> data sebelum proses akhir			
9.	Proses akhir hari			
10.	<i>Back up</i> data setelah proses akhir			
11.	Tutup sistem			
Akhir bulan				
1.	Proses perhitungan akhir bulan			
2.	Cetak laporan yang diperlukan			
3.	<i>Back up</i> data stlh perhitungan akhir bulan			
4.	Cetak laporan (daftar biaya meterai dicetak pada akhir tahun)			
5.	Proses re-valuasi			
6.	Cetak rekening koran			
7.	Proses akhir bulan			
8.	<i>Back up</i> data setelah proses akh-bul			
9.	Tutup sistem			
Catatan: Khusus akhir bulan, menu akhir hari nomor 6 di atas baru dilakukan setelah akhir bulan nomor 1 telah dilakukan.				

Gambar 4.3 Contoh Checklist dalam Aplikasi Giro