AUDIT SISTEM INFORMASI BERBASIS KOMPUTER

DIANA RAHMAWATI

Konsep Audit

Audit :

Sebuah proses sitematis untuk secara objektif mendapatkan dan mengevaluasi bukti mengenai pernyataan perihal tindakan dan transaksi bernilai ekonomi, untuk memastikan tingkat kesesuaian antara pernyataan tersebut denngan kriteria yanng telah ditetapkan serta mengkomunikasikan hsil-hasilnya pada para pemakai yang berkepentingan.

Tujuan Audit internal:

Untuk mengevaluasi kecukupan dan efektivitas sistem pengendalian intern perusahaan serta menetapkan keluasan dari pelaksanaan tanggung jawab yang benar-benar dilakukan.

Standar Audit Internal

IIA (*Institute of Internal Audit*) menetapkan 5 standar mengenai tanggung jawab auditor internal yaitu:

1. Melakukan tinjauan atas keandalan dan integritas informasi opersional dan keuangan serta bagaimana hal tersebut diidentifikasi , diukur, diklasifikasi dan dilaporkan.
2. Menetapkan apakah sistem telah didesain untuk sesuai dengan kebijakan operasional dan pelaporan, perencanaan, prosedur, hukum dan peraturan yang berlaku.
3. Melakukan tinauan mengenai bagaimana aset dijaga, dan memverifikasi keberadaan aset tersebut.
4. Mempelajari sumber daya perusahaan untuk menetapkan seberapa efektif dan efisien mereka digunakan.
5. Melakukan tinjauan atas operasional dan program perusahaan, untuk menetapkan apakah mereka telah dilaksanakan sesuai rencana dan apakah mereka dapat memenuhi tujuan mereka.

Jenis Kegiatan Audit

- **Audit Keuangan** :

  memerikasa keandalan dan integritas catatan –catatan akuntansi dan menghubungkannya dengan standar pertama dari kelima standar lingkup audit internal.

- **Audit Sistem Informasi:**

  melakukan tinjauan atas pengendalian SIA untuk menilai kesesuainnya dengan kebijakan dan prosedur pengendalian serta efektivitas dalam menjaga aset perusahaan. Lingkupnya secara kasar berhubungan dengan standar kedua dan ketiga dari IIA

- **Audit Operasional/Manajemen:**

  berkaitan dengan penggunaan secara ekonomis dan efisien sumber daya serta pencapaian sasaran dan tujuan yang telah ditetapkan. Lingkupnya berhubungan denngan standar keempat dan kelima.

Tinjauan Menyeluruh Proses Audit

Merencanakan Audit
Tetapkan lingkup dan tujuan; Organisisr tim audit; Kembangkan pengetahuan mengenai operasional bisnis; Tinjauan hasil audit audit sebelumnya;Identifikasi faktor-faktor resiko; Siapkan program audit.

Mengumpulkan Bukti Audit
Pengamatan atas kegiatan-kegiatan operasional; Tinjauan dokumentasi; Kuesioner: Berdiskusi dengan pegawai; Pemeriksaan fisik aset; Konfirmasi melalui pihak ketiga: Melakukan ulang prosedur; Pembuktian dengan dokumen sumber; Review analitis; Pengambilan sampel audit

Mengevaluasi Bukti Audit
Nilai kualitas pengendalian internal; Nilai keandalan informasi; Nilai kinerja Operasional; Pertimbangkankebutuhan atas bukti tambahan; Pertimbangkan faktor-faktor resiko; Pertimbangkan faktor materialitas; Dokumentasikan penemuan2 audit

Mengkomunikasikan Hasil Audit
Memformulasikan kesimpulan audit; Membuat rekomendasi bagi pihak manajemen; Mempersiapkan laporan audit; Menyajikan hasil-hasil audit kepada pihak manajemen

Pendekatan Audit Berdasarkan Resiko

1. Tentukan ancaman-ancaman yang dihadapi SIA
2. Identifikasi prosedur pengendalian
3. Evaluasi prosedur pengendalian
4. Evaluasi kelemahan yan tidak terungkap oleh prosedur pengendalian.

Tujuan Audit Sistem Informasi

Dalam melakukan audit sistem informasi auditor harus memastikan bahwa tujuan-tujuan berikut terpenuhi yaitu :

1. Perlengkapan keamanan melindungi perlengkapan komputer,program, komunikasi dan data dari akses yang tidak sah, modifikasi atau penghancuran.
2. Pengembangan dan perolehan program dilaksnakan sesuai dengan otorisasi khusus dan umum dari pihak manajemen.
3. Modifikasi program dilaksanakan dengan otorisasi dan persetujuan pihak manajemen.
4. Pemrosesan transaksi, file, laporan dan catatan komputer lainnya telah akurat dan lengkap
5. Data sumber yang tidak akurat atau yang tidak memiliki otorisasi yang tepat diidentifikasi dan ditangani sesuai dengan kebijakan manajerial yang telah ditetapkan.
6. File data komputer telah akurat, lengkap dan dijaga kerahasiaannya.

Frame Work For Auditing Computer Security

Types of Errors and Irregularities

- Accidental or intentional damage to hardware and files
- Unauthorized access to programs, data files, and other system resources
- Unauthorized disclosure of confidential data
- Theft or unauthorized modification of programs and data files
- Interruption of crucial business activities

Control Procedures

- Restrictions on physical access to computer equipment
- Logical access controls based on password protection
- *Encryption* of data during storage and transmission
- Virus protection procedures
- File backup and recovery procedures
- Fault-tolerant systems design
- *Disaster recovery planning*

Audit Procedures: System Review

- Inspect computer sites
- Interview IS personnel about security procedures
- Review written documentation about physical access policies and procedures
- Review logical access policies and procedures
- Review file backup and recovery policies and procedures
- Review procedures employed to minimize system downtime
- Examine system access logs
- Examine disaster recovery plan
- Examine casualty insurance policies

Audit Procedures: Tests of Controls

- Observe computer site access procedures
- Observe the preparation and off-site storage of backup files
- Review records of password assignment and modification
- Investigate how unauthorized access attempts were dealt with
- Verify the extent of data encryption use
- Verify the effective use of virus protection procedures
- Verify the use of preventive maintenance and uninterruptible power
- Verify amounts and limitations on insurance coverage
- Examine results of test simulations of disaster recovery plan

Compensating Controls

- Sound personnel policies
- Effective user controls
- Segregation of incompatible duties

Pengembangan Program

Dua hal yang dapat salah dalam pengembangan program yaitu :

1. Kesalahan yang tidak disengaja karena karena adanya kesalahpahaman atas spesifikasi sistem pemrograman.
2. Perintah yang tidak sah yang dengan sengaja dimasukkan kedalam program

Table 16.2 **Framework for Audit of Program Development**

Types of Errors and Irregularities

- Inadvertent programming errors
- Unauthorized program code

Control Procedures

- Management approval of programming specifications
- User approval of programming specifications
- Thorough testing of new programs
- User acceptance testing
- Complete systems documentation, including approvals

Audit Procedures: System Review

- Independent and concurrent review of systems development process
- Review systems development policies and procedures
- Review systems authorization and approval procedures
- Review programming evaluation standards
- Review program documentation standards
- Review program testing and test approval procedures
- Discuss systems development procedures with management, system users, and IS personnel
- Review final application system documentation

Audit Procedures: Tests of Controls

- Interview users about involvement in systems design and implementation
- Review minutes of development team meetings for evidence of involvement
- Verify user sign-off at milestone points in the development process
- Review test specifications, test data, and results of systems tests

Compensating Controls

- Strong processing controls
- Independent processing of test data by auditor

Table 16.3 Framework for Audit of Program Modification Procedures

Types of Errors and Irregularities

- Inadvertent programming errors
- Unauthorized program code

Control Procedures

- Listing of program components that are to be modified
- Management authorization and approval of program modifications
- User approval of program change specifications
- Thorough testing of program changes, including user acceptance test
- Complete program change documentation, including approvals
- Separate development, test, and production versions of program
- Changes implemented by personnel independent of users and programmers
- Logical access controls

Audit Procedures: System Review

- Review program modification policies, standards, and procedures
- Review documentation standards for program modification
- Review program modification testing and test approval procedures
- Discuss program modification policies and procedures with management, system users, and IS personnel
- Review final documentation for some typical program modifications
- Review test specifications, test data, and results of systems tests
- Review logical access control policies and procedures

Audit Procedures: Tests of Controls

- Verify user and IS management approval for program changes
- Verify that program components to be modified are identified and listed
- Verify that program change test procedures comply with standards
- Verify that program change documentation complies with standards
- Verify that logical access controls are in effect for program changes
- Observe program change implementation and verify that:
  - Separate development, test, and production versions are maintained
  - Changes are not implemented by either user or programming personnel
- To test for unauthorized or erroneous program changes, use:
  - Source code comparison program
  - Reprocessing
  - Parallel simulation

Compensating Controls

- Independent audit tests for unauthorized or erroneous program changes
- Strong processing controls

Table 16.4 Framework for Audit of Computer Processing Controls

Types of Errors and Irregularities

- Failure to detect incorrect, incomplete, or unauthorized input data
- Failure to properly correct errors flagged by data editing procedures
- Introduction of errors into master files during file updating
- Improper distribution or disclosure of computer output

Control Procedures

- Computer data editing routines
- Proper use of internal and external file labels
- Reconciliation of batch totals
- Effective error correction procedures
- Understandable operating documentation and run manuals
- Competent supervision of computer operations
- Effective handling of data input and output by data control personnel
- File change listings and summaries prepared for user department review
- Maintenance of proper environmental conditions in computer facility

Audit Procedures: System Review

- Review administrative documentation for processing control standards
- Review systems documentation for data editing and other processing controls
- Review operating documentation for completeness and clarity
- Review copies of error listings, batch total reports, and file change lists
- Observe computer operations and data control functions
- Discuss processing controls with operators and IS supervisory personnel

Audit Procedures: Tests of Controls

- Evaluate adequacy of processing control standards and procedures
- Evaluate adequacy and completeness of data editing controls
- Verify adherence to processing control procedures by observing computer operations and the data control function
- Verify that selected application system output is properly distributed
- Reconcile a sample of batch totals, and follow up on discrepancies
- Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling
- Verify processing accuracy for a sample of sensitive transactions
- Verify processing accuracy for selected computer-generated transactions
- Search for erroneous or unauthorized code via analysis of program logic
- Check accuracy and completeness of processing controls using test data
- Monitor on-line processing systems using concurrent audit techniques

Compensating Controls

- Strong user controls
- Effective source data controls

ble 16.5 Framework for Audit of Source Data Controls

ypes of Errors and Irregularities	
Inaccurate source data	• Unauthorized source data
ontrol Procedures	
Effective handling of source data input by data control personnel User authorization of source data input Preparation and reconciliation of batch control totals Logging of the receipt, movement, and disposition of source data input Check digit verification	• Key verification • Use of turnaround documents • Computer data editing routines • File change listings and summaries prepared for user department review • Effective procedures for correcting and resubmitting erroneous data
udit Procedures: System Review	
Review documentation about responsibilities of data control function Review administrative documentation for source data control standards Review methods of authorization and examine authorization signatures Review accounting systems documentation to identify source data content and processing steps and specific source data controls used	• Document accounting source data controls using input control matrix • Discuss source data control procedures with data control personnel, IS management, and system users
udit Procedures: Tests of Controls	
Observe and evaluate data control department operations and specific data control procedures Verify proper maintenance and use of data control log Evaluate how items recorded in the error log are dealt with	• Examine samples of accounting source data for proper authorization • Reconcile a sample of batch totals, and follow up on discrepancies • Trace disposition of a sample of errors flagged by data edit routines
ompensating Controls	
Strong user controls	• Strong processing controls

Framework for audit of data file control

Types of Errors and Irregularities	
• Destruction of stored data due to inadvertent errors, hardware or software malfunctions, and intentional acts of sabotage of vandalism	• Unauthorized modification or disclosure of stored data
Control Procedures	
• Secure file library and restrictions on physical access to data files • Logical access controls using passwords and access control matrix • Proper use of file labels and write-protection mechanisms • Concurrent update controls	• Use of data encryption for highly confidential data • Use of virus protection software • Maintenance of backup copies of all data files in an off-site location • Use of checkpoint and rollback to facilitate system recovery
Audit Procedures: System Review	
• Review documentation for functions of file library operation • Review logical access policies and procedures • Review operating documentation to determine prescribed standards for Use of file labels and write-protection mechanisms Use of virus protection software Use of backup data storage System recovery, including checkpoint and rollback procedures	• Review systems documentation to examine prescribed procedures for Use of concurrent update controls and data encryption Control of file conversions Reconciling master file totals with independent control totals • Examine disaster recovery plan • Discuss data file control procedures with IS managers and operators
Audit Procedures: Tests of Controls	
• Observe and evaluate file library operations • Review records of password assignment and modification • Observe and evaluate file-handling procedures by operations personnel • Observe the preparation and off-site storage of backup files • Verify the effective use of virus protection procedures	• Verify the use of concurrent update controls and data encryption • Verify completeness, currency, and testing of disaster recovery plan • Reconcile master file totals with separately maintained control totals • Observe the procedures used to control file conversion
Compensating Controls	
• Strong user controls • Effective computer security controls	• Strong processing controls

Computer Audit Software (CAS) atau *Generalized Audit Software* (GAS)

CAS :

Program komputer yang (berdasarkan spesifikasi dari auditor) menghasilkan program yang melaksanakan fungsi-fungsi audit.

CAS idealnya sesuai untuk :

- pemeriksaan file data yang besar
- Mengidentifikasi catatan-catatan yang membutuhkan pemeriksaan audit lebih lanjut.

Fungsi-Fungsi Umum Software Audit Komputer

- Pemformatan ulang
- Manipulasi file
- Perhitungan
- Pemilihan data
- Analisis data
- Pemrosesesan file
- Statistik
- Pembuatan laporan.

Audit Operasional Atas Suatu SIA

Langkah pertama adalah perencanaan audit, yaitu masa pembuatan lingkup dan tujuan audit, tinjauan awal atas sistem dilakukan dan program audit sementara dipersiapkan.

Selanjutnya pengumpulan bukti yang mencakup kegiatan-kegiatan:

1. Meninjau kebijakan dokumentasi operasional
2. Melakukan konfirmasi atas prosedur dengan pihak manajemen serta personil operasional
3. Mengamati fungsi-fungsi dan kegiatan operasional
4. Memeriksa rencana dan laporan keuangan serta operasional
5. Menguji akurasi informasi operasional
6. Menguji pengendalian.