INFORMATION SYSTEM AUDITING

By:

O. K. Ibedu (CGEIT, CISA)
Deputy Director, CBN

WAIFEM
Regional Course On Computer Applications In Accounting Auditing and Financial Management, Lagos, Nigeria.
(July 13th – 20th, 2009)
INFORMATION SYSTEM AUDITING

OUTLINE

- INTRODUCTION
- AUDITING IT INFRASTRUCTURE
- AUDITING OPERATIONS
- DATABASE REVIEW
- LOCAL AREA NETWORK REVIEW
- NETWORK OPERATING CONTROL REVIEW
- INFORMATION SYSTEM OPERATIONS REVIEW
- PROBLEM MANAGEMENT REPORTING REVIEWS
- HARDWARE AVAILABILITY AND UTILISATION REPORTING REVIEWS
- COMPUTER ASSISTED AUDITING TECHNIQUES (CAATS)
INTRODUCTION

Successful leaders understand that IT serves the business. Performance measurement, auditing and reporting are as important to IT as they are to any business. Routine audit, critical evaluation of initiatives, coupled with expert management, can transform IT into a strategic asset. IT transformation is about more than technological innovation; it is about innovation that brings real business value to organizations. It improves decision making, eliminates redundancies and saves money. As a partner to business, IT should maximize the power of a company’s investments and minimize related operational expenses.

Aligning IT processes to business goals streamlines operations. The key to IT success is its ability to deliver initiatives against strategy and to communicate results.

a)  AUDITING IT INFRASTRUCTURE

Hardware Reviews:

(i) Review of the Capacity Management Policy and procedures for hardware and performance evaluation procedures to determine:

- Whether the procedure in place will ensure continuous review of hardware and system software performance and capacity.
- Whether the criteria issued in the performance monitoring plan are based on historical data obtained from problem logs, processing schedules, accounting system reports, preventive maintenance schedules and reports.

(ii) Review the hardware acquisition plan to determine:

- Whether the hardware acquisition plan is compared to business plan.
• Whether the environment is adequate for the current installed hardware and provision made for new hardware to be added under the approved acquisition plan.
• Whether the acquisition plan has taken into consideration deficiencies noted in the former.
• Whether the acquisition plan has taken into consideration technological obsolescence of the installed equipment, as well as the new equipment in the plan.
• The adequacy of documentation for hardware and software specifications, installation requirements and the likely lead-time associated with planned acquisitions.

(iii) Review the Microcomputer (PC) Acquisition Criteria to determine:
• Whether Management has issued written policy statements regarding the acquisition and use of PCs and that these statements have been communicated to the users.
• Criteria for acquisition of PCs has been developed and that procedures have been established to facilitate the acquisition approval process.
• Requests for acquisition of PCs are supported by cost benefit analysis.
• All PCs are purchased through the IS purchasing department to take advantage of volume discounts and standardization.

(iv) Review Change Management Controls for the following:
• Determine if the individual responsible for scheduling was advised in a timely manner regarding changes to hardware configuration.
• Verify that information system management has developed and enforced change, schedules that allow time for adequate installation and testing of new hardware.
Verify that the operator documentation used in the information system department is appropriately revised prior to implementation of changes in hardware.

Select a sample of hardware changes that have affected the scheduling of processing and determine if the plans for changes were addressed in a timely manner.

Ascertain that all hardware changes have been communicated to the system programmers, application programmers and the information system staff to ensure that changes and tests are coordinated properly.

Evaluate the effectiveness of changes to assure that they do not interfere with normal application production processing.

(b) OPERATING SYSTEM REVIEWS

When auditing operating software development, acquisition or maintenance, the following approach may be adopted:

i) Interview technical service and other personnel regarding:
   - Review and approval process of option selection
   - Test procedures for software implementation.
   - Review and approval procedures for test results
   - Implementation procedures
   - Documentation requirements.

ii) Review system software selection procedures to determine that they:
   - Address both, the Information System (IS) requirements and business plans.
   - Include IS processing and control requirements.
   - Include an overview of the capabilities of the software and control options.

iii) Review the feasibility study and selection process to determine the following:
• Proposed system objectives and purposes are consistent with the request for proposal.
• Same selection criteria are applied to all proposals.

iv) Review cost/benefit analysis of system software procedures to determine they have addressed the following areas:
• Direct financial costs associated with the product.
• Cost of Product Maintenance.
• Hardware requirements and capacity of the products.
• Training and technical support requirements.
• Impact of the product on processing reliability.
• Impact on data security.
• Financial stability of the vendor's operations.

v) Review controls over the installation of changed system software to determine the following:
• That all appropriate levels of software have been implemented and that predecessor updates have taken place.
• System software changes are scheduled when they least impact transaction processing.
• A written plan is in place for testing changes to system software.
• Tests are being completed as planned.
• Problems encountered during testing were resolved and the changes were re-tested.
• Test procedures are adequate to provide reasonable assurance that changes applied to the system correct known problems and do not create new problems.
• Software will be identified before it is placed into the production environment.
• Fallback or restoration procedures are in place in case of production failure.
vi) Review system software maintenance activities to determine the following:
   - Changes made to the system software are documented.
   - Current versions of the software are supported by the vendor.
   - Vendors maintenance activities are logged.

vii) Review system software change controls to determine the following:
    - Access to the libraries containing the system software is limited to individuals needing to have such access.
    - Changes to the software must be adequately documented and tested prior to implementation.
    - Software must be properly authorized prior to moving from the test environment to the production environment.

eiii) Review systems documentation specifically in the areas of:
     - Installation control statements.
     - Parameter tables.
     - Exit definitions.
     - Activity logs/reports.

ix) Review and test systems software implementation to determine the adequacy of controls in:
    - Change procedures.
    - Authorization procedures.
    - Access security features.
    - Documentation requirements.
    - Documentation of system testing.
    - Audit trails.
    - Access controls over the software in production.

x) Review authorization documentation to determine whether:
    - Additions, deletions or changes to access authorization have been documented.
• Attempted violation reporting and follow-up have been documented.

xi) Review system software security for the following:
• Procedures have been established to restrict the ability to circumvent logical security access control.
• Procedures have been established to limit access to the system interrupt capability.
• Security provided by the system software.
• Existing physical and logical security provisions are adequate to restrict access to the master consoles.
• System Software vendor-supplied installation passwords were changed at the time of installation.

xii) Review database supported information systems controls to determine the following:
• Access to shared data is appropriate.
• Data organization is appropriate.
• Adequate change procedures are utilized to ensure the integrity of the database management software.
• Integrity of the database management system’s data dictionary is maintained.
• Data redundancy is minimized by the database management system where redundant data exists, appropriate cross-referencing is maintained within the system’s data dictionary or other documentation.

(c ) DATABASE REVIEW.

An IS auditor should review design, access, administration, interfaces and portability when auditing a database.
(i) DATABASE DESIGN

- IS Auditor should verify the existence of a database model, that all entities have a significant name and identified primary and foreign keys.
- Verify that the relations have explicit cardinality, coherent and significant names and that the business rules are expressed in the diagram.
- Finally, verify that the entity-relation model is synchronized with the database's physical scheme.
- Review the logical scheme to ensure all entities in the entity-relation diagram exist as tables or views.
- All relations should be represented through primary or foreign keys and all attributes should have a logical name, an indicator specifying it as a primary or foreign key and an indicator of whether null values are allowed or not.
- Nulls should not be allowed for primary keys, while nulls for foreign keys could be with the cardinality expressed in the entity-relation model.
- The physical scheme should be reviewed for allocation of initial and extension space (storage) for tables, logs, indexes, and temporary areas. Indexes by primary key and frequency of access should exist. If the database in not normalized, the justification should be reviewed.

ii) DATABASE ACCESS:

- The IT Auditor should analyze the main access to the database, stored procedures and triggers, verify that the use of indexes minimize access time and that open searches, if not based in indexes are justified. If the database management system (DBMS) allows the selection of the methods or types of indexes, the correct use should be verified.
iii) DATABASE ADMINISTRATION:
   o The IT Auditor should verify that the security levels for all users and their roles are identifiable within the database and access rights for all users and/or group of users are justified.
   o The Auditors should also confirm that back-up and disaster recovery procedures exist to assure the reliability and availability of the database.
      • The Auditor should also confirm that backup and disaster recovery procedures put in place to assure the adequate handling of consistency and integrity during concurrent accesses should be collaborated by the IT Auditor.

iv) DATABASE INTERFACES:
   • To ensure the security and confidentiality of data, information import and export procedures with other systems should be verified by the Auditor.

v) DATABASE PORTABILITY:
   • Verify that, whenever possible structured Query Language (SQL) is used.

(d) LOCAL AREA NETWORK (LAN) REVIEWS

The IS Auditor should review controls over LANs to ensure that standards are in place for designing and selecting a LAN architecture and for ensuring that the costs of procuring and operating the LAN do not exceed the benefits.

To effectively perform an audit review of LAN, the IS auditor should identify the following:

• LAN topology and network design.
• Significant LAN components such as servers and modems.
Network topology (including internal LAN configuration as well as interconnections to other LANs, WAN or public networks)
LAN uses (including significant traffic types and main applications used over the network).
LAN administrator.
Significant groups of LAN users.
In the IS Auditor should gain understanding of the following:
= Functions performed by the LAN administrator
= Departmental procedures and standards relating to network design, support, naming conventions and data security.
LAN transmission media and techniques including bridges, routers, gateways and switches. The IS Auditor should be able to make an assessment of the significant threats to the LAN with good understanding of the subjects discussed above. The IS Auditor should evaluate the controls used to minimize the risks.

(e) NETWORK OPERATING CONTROL REVIEWS:

An IS Auditor should review the network operations controls to determine that:

Appropriate implementation conversion and acceptance test plans were developed for the distributed data processing network.
Implementation and testing plans for the network’s hardware and communication links were established.
Operating provisions for distributed data processing networks exist to ensure consistency with the laws and regulations governing transmission of data.
Procedures to ensure compatibility are properly applied to all the networks datasets and that their requirements for their security have been determined.
All sensitive files/datasets in the network have been identified and that the requirements for their security have been determined.
• Procedures were established to assure effective controls over the hardware and software used by the departments served by the distributed processing network.
• Adequate restart and recovery mechanisms have been installed at every user location served by the distributed processing networks.
• The IS distributed network has been designed to assure that failure of service at any one site will have a minimal effect on the continued service to other sites served by the network.
• All changes made at the user sites or by IS management to the operating systems software used by the network are controlled and can be detected promptly by the network administrator or those responsible for the network.
• Individuals have access only to authorized applications, transaction processors and data sets.
• System commands affecting more than network site are restricted to one terminal and to an authorized individual with an overall network control responsibility and security clearance.
• Encryption is being used in the network for sensitive data.
• Appropriate security policies and procedures have been implemented in one of the following environments:

  = Highly Distributed – IS security under the control of individual user management?
  = Distributed - IS security under the direction of user management, but adheres to the guidelines established.
  = Mixed - IS security under the direction of individual user management but the overall responsibility remains with IS management.
  = Centralized - IS security under the direction of IS management, but it maintains a close relationship with user management?
  = Highly centralized - IS security under the complete control of IS management?
(f) IS OPERATIONS REVIEW

Audit procedures should include observations of IS personal performing their duties to determine whether controls are in place to ensure efficiency of operations, adherence to established standards and policies, adequate supervision, IS management review and data integrity and security.

- Computer operations control

This relate to day-today operation of the hardware and software with the IS department, responsibility for the running of the computers including the mounting of files located on secondary storage media, and discontinuance of the use of devices requiring maintenance.

Computer operations control include the following:

- **Restricting Operator access capabilities:**
  - Operators should have restricted access to files and documentation libraries.
  - Operator responsibilities should be limited to the running of the computer and related peripheral equipment.
  - Operators should be restricted from correcting program and data problems.
  - Operators should have restricted access to utilities that allow system fixes to software and or data.
  - Operators should have limited access to production source code and data libraries, including run procedures.

- **SCHEDULING**
  - Operations should record jobs that are to be processed and their required data files.
  - Operations should schedule jobs for processing on a predetermined basis and perform them using either automated scheduling software or a manual schedule.
- Using exception processing procedures to obtain written or electronic approval from application owners to run jobs or programs in another sequence:
  - Operators should obtain written or electronic approval from owners when scheduling on request only jobs.
  - Operators should record all exception processing requests.
  - Operators should review the exception processing request log to determine the appropriateness of procedures performed.

= EXECUTING RE-RUN HANDLING:
  - All re-execution of jobs should be properly authorized and logged for IS management review.
  - Procedures should be established for re-running jobs to ensure the correct input files are used and that subsequent jobs in the sequence are also re-run if appropriate.

= IS operations audit procedures should include a review of the operator manuals to determine whether instructions are adequate to address the operation of the computer and its peripheral equipment, start-up and shutdown procedures actions to be taken in the event of machine/program failure, records to retained, routine job duties and restricted activities.

In addition, the IS Auditor should conduct tests to determine whether these procedures are being followed in accordance with management's intent and authorization.

= LIBRARIAN ACCESS CAPABILITIES
  - Librarian should not have main application hardware access.
  - Librarian should only have access to the tape management system.
  - Access to Library facilities should be restricted to authorized staff.
  - Removal of files should be restricted by production scheduling software.
- Librarian should handle the receipt and return of foreign media entering the Library.
- Logs of the sign-in and sign-out of data files and media should be maintained.

## CONTENTS AND LOCATION OF OFF-LINE STORAGE:

- Off-line file storage media containing production system programs and data should be clearly marked as to content.
- Off-line library facilities should be located away from the computer room. Audit procedures should include a review of policies and procedures for:
  - Administering the off-line library
  - Checking out/in tape media including signature authorizations
  - Identifying, labeling, delivering and retrieving off-site backup files.
  - Inventorying the system for on-site and off-site tapes including specific storage locations of each tape.
  - Scratching, deleting and securing disposal/destruction of tape datasets including signature authorizations.

## FILE HANDLING

The IT Auditor should ensure that procedures exist to control the receipt and release of files/secondary storage media to/from other locations. Internal tape labels should be used to help ensure the correct tapes are mounted for processing.

Audit procedures should include a review of these procedures to determine whether they are adequate and in accordance with management’s intent and authorization. In addition, the IS Auditor should test to determine whether these procedures are being followed.

## DATA ENTRY CONTROL

Data entry function is performed by the data owner and the major controls include:
- Authorization of input documents.
- Reconciliation of batch totals.
- Segregation of duties between the person who keys the data and the person who reviews the keyed data for accuracy and errors.

Audit procedures for data entry should include a review of the controls and the procedures to determine whether:

- Adequate controls exist.
- IS personnel are adhering to the established policies.
- Proper segregation of duties is being maintained.
- Control reports are being produced, maintained and reviewed.
- The control reports are accurate and complete.
- Authorization forms are complete and contain appropriate signatures.

Light out operations is the automation of key computer room operations whereby tasks can take place without human intervention. The types of tasks being automated with the use of system operations software are:

- Job scheduling.
- Console operation.
- Report balancing and distribution.
- Re-run/re-start activities.
- Tape mounting and management.
- Storage device management.
- Environmental monitoring.
- Physical and data security.

Several control concerns arise from a lights out operation. These concerns include the following:

- Remote access to the master console is often granted to stand-by operators for contingency purposes such as a failure in the automated software. Therefore, communication access is opened to allow for very risky, high-powered console commands. Communication access security must be extensive. This would include using leased lines and dial-back capabilities.
• Contingency plans must allow for the proper identification of a disaster in the unattended facility. In addition, the automated operation software or manual contingency procedures must be adequately documented and attested at the recovery site.
• Since vital IS operations are performed by software systems, proper program change controls and access controls need to be applied to this software. Testing of the software should also performed on a periodic basis especially when changes or updates are applied.
• Ensure that errors are not hidden by the software and that all errors result in operator notification.

(g) PROBLEM MANAGEMENT REPORTING REVIEWS
The IS Auditor should ensure adequate and documented procedures have been developed to guide IS operations personnel in logging, analyzing, resolving and escalating problems in a timely manner in accordance with management’s intent and authorization.

The IS Auditor should perform procedures to ensure that the problems management mechanism is being properly maintained and that outstanding errors are being adequately addressed and resolved in a timely manner. These procedures include:

• Interviews of IS operations personnel.
• Reviews of the procedures used by the IS department for recording, evaluating and resolving or escalating any operating or processing problems to determine whether they are adequate for service analysis.
• Reviews of the performance records to determine whether problems exist during processing.
• Reviews of the reasons for delays in application program processing to determine whether they are valid.
• Reviews of the procedures used by the IS department to collect statistics regarding online processing performance to determine whether the analysis is accurate and complete.
• Determination that the IS department has established procedures for handling data processing problems.
• Determination that all problems identified by IS operations are being recorded for verification and resolution.
• Determination that significant and recurring problems have been identified and actions are being taken to prevent their reoccurrence.
• Determination that processing problems were resolved on a timely basis and the resolution was complete and reasonable.
• Reviews of IS management reports produced by the problem management system to ensure evidence of proper management review.
• Reviews of outstanding error-log entries describing problems to be resolved for proper documentation and to ensure that they are being addressed in a timely manner.
• Reviews of operations documentation to ensure that procedures have been developed for the escalation of unresolved problems to a higher level of IS management.

(h) HARDWARE AVAILABILITY AND UTILIZATION

Reporting Reviews:

Hardware availability and utilization can be obtained from the problem log, processing schedules, job accounting system reports, preventive maintenance schedules and reports and the hardware performance monitoring plan.

Some of the audit procedures to perform to determine, whether proper reporting of system activities occurs to ensure optimal hardware availability and utilization include:

• Review the hardware performance monitoring plan and compare it with the problem log, processing schedules, job accounting system reports, preventive maintenance schedules and reports to determine the validity of the process.
• Review the problem log to determine whether hardware malfunctions, re-runs, the use of software utilities, abnormal system terminations and operator actions have been reviewed by IS management.

• Review the preventive maintenance schedule to determine if the prescribed maintenance frequency recommended by the respective hardware vendors is being observed.

• Review the preventive maintenance schedule to verify that maintenance is not done during peak workload periods, thereby avoiding impairment of hardware availability.

• Review the preventive maintenance schedule to determine that it is not being performed while the system is processing critical or sensitive applications.

• Review the control and management of equipment that has the ability to contact its manufacturer without manual intervention in case of equipment failure.

• Review the hardware availability and utilization reports to determine that scheduling is adequate to meet workload schedules and user requirements.

• Review the workload schedule and the hardware availability and utilization reports to determine that scheduling is sufficiently flexible to accommodate required hardware preventive maintenance.

• Determine whether IS resources are readily available for processing those application programs which require a high level of resource availability.

(i) COMPUTER ASSISTED AUDIT TECHNIQUES (CAATS)

The IS Audit should have a thorough understanding of computer assisted audit techniques and know where and when to apply them. This understanding should include both the use of generalized audit software and other techniques such as test data generators and integrated test facility techniques.
In addition to selecting the appropriate techniques, the IS Auditor should understand the importance of documenting the results of such tests for audit evidence purposes.

Examples of the use of CAATS are:

- **Test Data Generators:**
  Prepare a computerized test data file for use in testing and verifying the logic of application programs.

- **Expert system:**
  Software applications developed to hold a base of expert knowledge and logic provided by experts in a given field. Such a software application permits the computerized use of the decision-making process of these experts.

- **Standard utilities:**
  Resident in software packages that specify the status of parameters used to install the package.

- **Software Library packages:**
  Verify the integrity and appropriateness of program changes.

- **Integrated Test facilities:**
  Involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

- **SNAPSHOT:**
  This technique involves taking "pictures" of a transaction as it flows through the computer system. Audit software routines are embedded at different points in the processing logic to capture images of the transaction as it progresses through the various stages of processing. Such a technique permits the IS Auditor to track data and evaluates the computer process applied to this data throughout the various stages of processing.
• System control Audit Review File:

Involves embedding audit software modules within an application system to provide continuous monitoring of the system’s transactions. The information is collected into a special computer file that can be examined by the IS Auditors.

• SPECIALIZED AUDIT SOFTWARE:

Used to perform specific audit steps for the IS Auditor, such as sampling, footing and matching etc.

Advantages of CAATs

• Reduced level of audit risk.
• Greater independence from the auditee
• Broader and more consistent audit coverage.
• Faster availability of information.
• Improved exception identification.
• Greater flexibility of run times.
• Greater opportunity to quantify internal control weaknesses.
• Enhanced sampling.
• Cost savings over time.

The IS Auditor should weigh the cost/benefit of CAATs before going through the effort time and expense of purchasing or developing them.

Issues to consider include:

• Ease of use, both for existing audit staff and future staff.
• Training requirement.
• Complexity of coding and maintenance.
• Flexibility of uses.
• Installation requirements.
• Processing efficiency (especially with a PC CAAT)
• Effort required to bring the source data into CAATs for analysis.
The following documentation should be retained when developing CAATs.

- Commented program listing.
- Flowcharts, both detailed and overview.
- Integrated Test facilities:
- Sample reports
- Record and file layouts.
- Field definitions.
- Operating instructions.
- Description of applicable source documents.

The CAATs documentation should be referenced to the audit program and clearly identify the audit procedures and objectives being served. The IS Audit should request read-only access to production data for use with CAATs. Any data manipulation done by the IS Auditor should be done on copies of production files in a controlled environment that ensures production data are not exposed to unauthorized updating.