Accounting Information Systems

9th Edition

Marshall B. Romney

Paul John Steinbart

Auditing of Computer-Based Information Systems

Chapter 10

Learning Objectives

1 Describe the scope and objectives of audit work, and identify the major steps in the audit process.

2 Identify the objectives of an information system audit, and describe the four-step approach necessary for meeting these objectives.

Learning Objectives

3 Design a plan for the study and evaluation of internal control in an AIS.

4 Describe computer audit software, and explain how it is used in the audit of an AIS.

5 Describe the nature and scope of an operational audit.

Introduction

- Seattle Paper Products (SPP) is modifying its sales department payroll system to change they way it calculates sales commissions.
- Jason Scott was assigned to use the audit software to write a parallel simulation test program to calculate sales commissions.
- Jason’s calculations were $5,000 less than those produced by SPP’s new program.

Introduction

- He selected a salesperson for whom there was a discrepancy and recalculated the commission by hand.
- The result agreed with his program.
- Jason is now convinced that his program is correct and that the error lies with the new program.

Introduction

Jason ponders the following questions:

- How could a programming error of this significance be overlooked by experienced programmers who thoroughly reviewed and tested the new system?
- Is this an inadvertent error, or could it be another attempted fraud?
- What can be done to find the error in the program?

Introduction

- This chapter focuses on the concepts and techniques used in auditing an AIS.
- It is written primarily from the perspective of the internal auditor.
- The chapter presents a methodology and a set of techniques for evaluating internal controls in an AIS.
- Finally, operational audits of an AIS are reviewed.

Learning Objective 1

Describe the scope and objectives of audit work, and identify the major steps in the audit process.

The Nature of Auditing

- The American Accounting Association defines auditing as follows:
- *Auditing* is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users.

The Nature of Auditing

- Auditing requires a step-by-step approach characterized by careful planning and judicious selection and execution of appropriate techniques.
- Auditing involves the collection, review, and documentation of audit evidence.

Internal Auditing Standards

- According to the Institute of Internal Auditors (IIA), the purpose of an internal audit is to evaluate the adequacy and effectiveness of a company’s internal control system.
- Also, it is to determine the extent to which assigned responsibilities are actually carried out.

Internal Auditing Standards

- The IIA’s five audit scope standards are:
  1. Review the reliability and integrity of operating and financial information and how it is identified, measured, classified, and reported.
  2. Determine whether the systems designed to comply with operating and reporting policies, plans, procedures, laws, and regulations are actually being followed.

Internal Auditing Standards

3 Review how assets are safeguarded, and verify the existence of assets as appropriate.

4 Examine company resources to determine how effectively and efficiently they are utilized.

5 Review company operations and programs to determine whether they are being carried out as planned and whether they are meeting their objectives.

Types of Internal Auditing Work

- What are the three different types of audits commonly performed?
  1. Financial audit
  2. Information system (IS) audit
  3. Operational or management audit

Types of Internal Auditing Work

- The *financial audit* examines the reliability and integrity of accounting records (both financial and operating information).
- The *information systems (IS) audit* reviews the general and application controls in an AIS to assess its compliance with internal control policies and procedures and its effectiveness in safeguarding assets.

Types of Internal Auditing Work

- The *operational, or management, audit* is concerned with the economical and efficient use of resources and the accomplishment of established goals and objectives.

An Overview of the Auditing Process

- All audits follow a similar sequence of activities and may be divided into four stages.
  1. Audit planning
  2. Collection of audit evidence
  3. Evaluation of audit evidence
  4. Communication of audit results

An Overview of the Auditing Process

Audit Planning

Establish scope and objectives

Organize audit team

Develop knowledge of business operations

Review prior audit results

Identify risk factors

Prepare audit program

An Overview of the Auditing Process

Collection of Audit Evidence

Observation of operating activities
Review of documentation
Discussion with employees and questionnaires
Physical examination of assets
Confirmation through third parties
Reperformance of procedures
Vouching of source documents
Analytical review and sampling

An Overview of the Auditing Process

Evaluation of Audit Evidence
Assess quality of internal controls
Assess reliability of information
Assess operating performance
Consider need for additional evidence
Consider risk factors
Consider materiality factors
Document audit findings

An Overview of the Auditing Process

Communication of Audit Results

Formulate audit conclusions

Develop recommendations for management

Present audit results to management

Learning Objective 2

Identify the objectives of an information system (IS) audit, and describe the four-step approach necessary for meeting these objectives.

Information Systems Audits

- The purpose of an AIS audit is to review and evaluate the internal controls that protect the system.
- When performing an IS audit, auditors should ascertain that the following objectives are met:
  1. *Security* provisions protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.

Information Systems Audits

2 *Program development* and acquisition is performed in accordance with management's general and specific authorization.

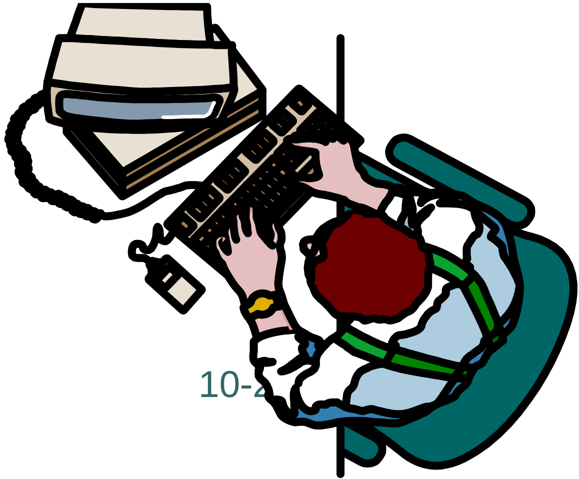
3 *Program modifications* have the authorization and approval of management.

4 *Processing* of transactions, files, reports, and other computer records is accurate and complete.

Information Systems Audits

5 *Source data* that are inaccurate or improperly authorized are identified and handled according to prescribed managerial policies.

6 *Computer data files* are accurate, complete, and confidential.



The Risk-Based Audit Approach

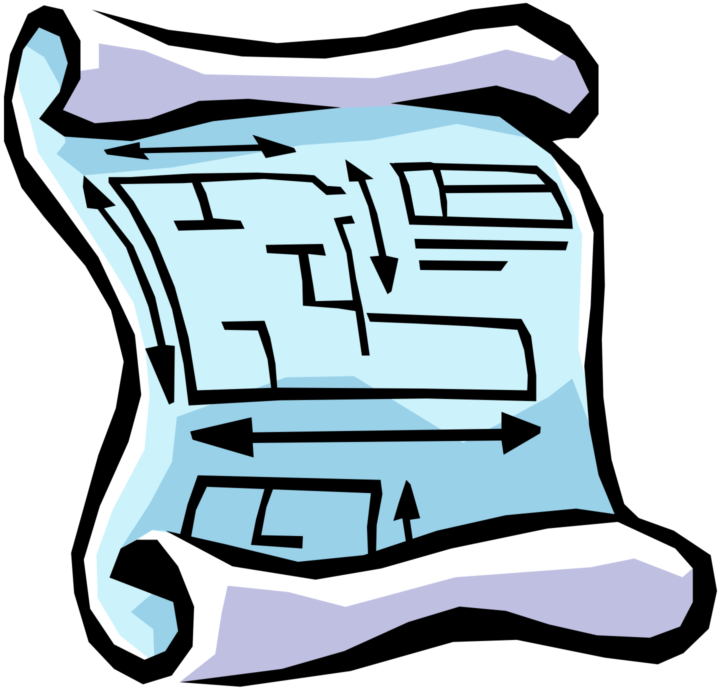
- The risk-based approach to auditing provides auditors with a clear understanding of the errors and irregularities that can occur and the related risks and exposures.
- This understanding provides a sound basis for developing recommendations to management on how the AIS control system should be improved.

The Risk-Based Audit Approach

- What is the four-step approach to internal control evaluation?
  1. Determine the threats facing the AIS.
  2. Identify the control procedures that should be in place to minimize each threat.
  3. Evaluate the control procedures.
  4. Evaluate weakness (errors and irregularities not covered by control procedures).

Learning Objective 3

Design a plan for the study and evaluation of internal control in an AIS.



Framework for Audit of Computer Security (Objective 1)

Some types of security errors and fraud:

- theft of accidental or intentional damage to hardware and files
- loss, theft, or unauthorized access to programs, data files; or disclosure of confidential data
- unauthorized modification or use of programs and data files

Framework for Audit of Computer Security (Objective 1)

Some types of control procedures:

- developing an information security/protection plan, and restricting physical and logical access
- encrypting data and protecting against viruses
- implementing firewalls
- instituting data transmission controls, and preventing and recovering from system failures or disasters

Framework for Audit of Computer Security (Objective 1)

Some systems review audit procedures:

- inspecting computer sites
- interviewing personnel
- reviewing policies and procedures
- examining access logs, insurance policies, and the disaster recovery plan

Framework for Audit of Computer Security (Objective 1)

Some tests of control audit procedures:

- observing procedures
- verifying that controls are in place and work as intended
- investigating errors or problems to ensure they were handled correctly
- examining any test previously performed

Framework for Audit of Computer Security (Objective 1)

Some compensating controls:

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

Framework for Audit of Program Development (Objective 2)

Some types of errors and fraud:

- Inadvertent programming errors
- Unauthorized program code

Framework for Audit of Program Development (Objective 2)

Some types of control procedures:

- Management authorization for program development and approval of programming specifications
- User approval of programming specifications
- Thorough testing of new programs and user acceptance testing
- Complete systems documentation

Framework for Audit of Program Development (Objective 2)

Some systems review audit procedures:

- Independent and concurrent review of systems development process
- Systems review of development policies, authorization, and approval procedure
- Programming evaluation and documentation standards, and program testing and test approval procedures

Framework for Audit of Program Development (Objective 2)

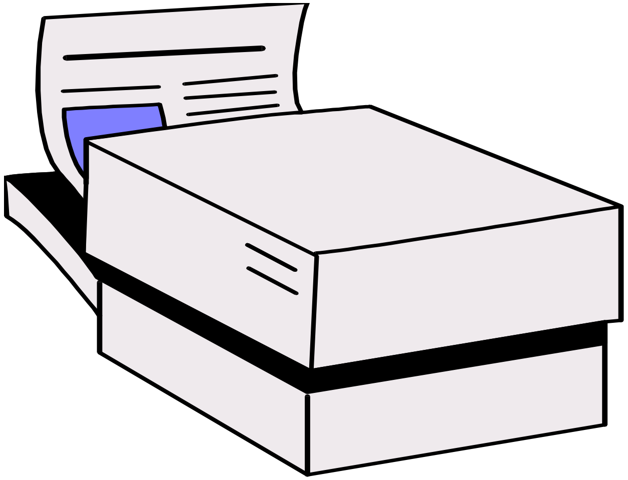
Some tests of control audit procedures:

- User interviews about involvement in systems design and implementation
- Reviewing minutes of development team meetings for evidence of involvement
- Verifying management and user sign-off at milestone points in the development process
- Reviewing test specifications, data, and results

Framework for Audit of Program Development (Objective 2)

Some compensating controls:

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



Framework for Audit of Program Modifications (Objective 3)

- *Some types of errors and fraud:*
  - Inadvertent programming errors
  - Unauthorized program code
- These are the same as in audit program development.

Framework for Audit of Program Modification Procedures (Objective 3)

Some types of control procedures:

- Listing of program components that are to be modified, and management authorization and approval of programming modifications
- User approval of program changes specifications
- Thorough testing of program changes, including user acceptance test

Framework for Audit of Program Modification Procedures (Objective 3)

Some systems review audit procedures:

- Reviewing program modification policies, standards, and procedures
- Reviewing documentation standards for program modification, program modification testing, and test approval procedures
- Discussing systems development procedures with management

Framework for Audit of Program Modification Procedures (Objective 3)

Some tests of control audit procedures:

- Interviewing users about involvement in systems design and implementation
- Reviewing minutes of development team meetings for evidence of involvement
- Verifying management and user sign-off at milestone points in the development process
- Reviewing test specifications, data, and results

Framework for Audit of Program Modification Procedures (Objective 3)

- *Some compensating controls:*
  - Strong processing controls
  - Independent processing of test data by auditor
- These are the same as in audit program development.

Framework for Audit of Computer Processing Controls (Objective 4)

- *Some types of errors and fraud:*
  - Failure to detect incorrect, incomplete or unauthorized input data
  - Failure to properly correct errors flagged by data editing procedures
  - Introduction of errors into files or databases during updating

Framework for Audit of Computer Processing Controls (Objective 4)

- *Some types of control procedures:*
  - Computer data editing routines
  - Proper use of internal and external file labels
  - Effective error correction procedures
  - File change listings and summaries prepared for user department review

Framework for Audit of Computer Processing Controls (Objective 4)

- *Some systems review audit procedures:*
  - Review administrative documentation for processing control standards
  - Observe computer operations and data control functions
  - Review copies of error listings, batch total reports and file change list

Framework for Audit of Computer Processing Controls (Objective 4)

- *Some tests of control audit procedures:*
  - Evaluation of adequacy and completeness of data editing controls
  - Verify adherence to processing control procedure by observing computer operations and the data control function
  - Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling
  - Monitor on-line processing systems using concurrent audit techniques

Framework for Audit of Computer Processing Controls (Objective 4)

- *Some compensating controls:*
  - Strong user controls
  - Effective source data controls

Framework for Audit of Source Data Controls (Objective 5)

- *Some types of errors and fraud:*
  - Inadequate source data
  - Unauthorized source data
- *Some types of control procedures:*
  - User authorization of source data input
  - Effective handling of source data input by data control personnel
  - Logging of the receipt, movement, and disposition of source data input
  - Use of turnaround documents

Framework for Audit of Source Data Controls (Objective 5)

- *Some systems review audit procedures:*
  - Reviewing documentation for source data control standards
  - Document accounting source data controls using an input control matrix
  - Reviewing accounting systems documentation to identify source data content and processing steps and specific source data controls used.

Framework for Audit of Source Data Controls (Objective 5)

- *Some tests of control audit procedures:*
  - *Observation and evaluation of data control department*
  - *Reconciliation of a sample of batch totals and follow up on discrepancies*
  - Examination of samples of accounting source data for proper authorization
- *Some compensating controls:*
  - Strong processing controls
  - Strong user controls

Framework for Audit of Data File Controls (Objective 6)

- *Some types of errors and fraud:*
  - Unauthorized modification or disclosure of stored data
  - Destruction of stored data due to inadvertent errors, hardware or software malfunctions and intentional acts of sabotage or vandalism

Framework for Audit of Data File Controls (Objective 6)

- *Some types of control procedures:*
  - Concurrent update controls
  - Proper use of file labels and write-control mechanisms
  - Use of virus protection software

Framework for Audit of Data File Controls (Objective 6)

- *Some systems review audit procedures:*
  - Examination of disaster recovery plan
  - Discussion of data file control procedures with systems managers and operators
  - Review of logical access policies and procedures
  - Review of documentation for functions of file library operation

Framework for Audit of Data File Controls (Objective 6)

- *Some tests of control audit procedures:*
  - Observing and evaluating file library operations
  - Review records of password assignment and modification
  - Observation of the preparation of off-site storage back-up facilities
  - Reconciliation of master file totals with separately maintained control totals
- *Some compensating controls:*
  - Effective computer security controls
  - Strong user controls
  - Strong processing controls

Learning Objective 4

Describe computer audit software, and explain how it is used in the audit of an AIS.

Computer Software

- A number of computer programs, called computer audit software (CAS) or generalized audit software (GAS), have been written especially for auditors.
- CAS is a computer program that, based on the auditor’s specifications, generates programs that perform the audit functions.

Usage of Computer Software

- The auditor’s first step is to decide on audit objectives, learn about the files to be audited, design the audit reports, and determine how to produce them.
- This information is recorded on specification sheets and entered into the system via a data entry program.

Usage of Computer Software

- This program creates specification records that the CAS uses to produce one or more auditing programs.
- The auditing programs process the sources files and perform the auditing operations needed to produce the specified audit reports.

General Functions of Computer Audit Software

- Reformatting
- File manipulation
- Calculation
- Data selection
- Data analysis
- File processing
- Statistics
- Report generation

Learning Objective 5

Describe the nature and scope of an operational audit.

Operational Audits of an AIS

The techniques and procedures used in operational audits are similar to those of IS and financial audits.

- The basic difference is that the IS audit scope is confined to internal controls, whereas the financial audit scope is limited to IIS output.
- The operational audit scope encompasses all aspects of IS management.

Operational Audits of an AIS

- Operational audit objectives include evaluating effectiveness, efficiency, and goal achievement.
- What are some evidence collection activities?
  - Reviewing operating policies and documentation
  - Confirming procedures with management and operating personnel

Operational Audits of an AIS

Evidence collection procedures, cont.

- Observing operating functions and activities
- Examining financial and operating plans and reports
- Testing the accuracy of operating information
- Testing controls

Case Conclusion

- Under the new commission policy, the commission rate changes when sales for the period exceed $40,000.
- Jason discovered a commission rate of 0.085 for sales in excess of $40,000, while the policy called for only 0.075.
- This was the source of the differences between the two programs.
- There was a coding error.

End of Chapter 10