

Auditing Computer-Based Information Systems

Source:

Romney/Steinbart AIS 11th ed & CISA Review, ISACA
Anotasi diagram/gambar penjelasan oleh Arrianto Mukti Wibowo

- ❖ Questions to be addressed in this session include:
 - What are the scope and objectives of audit work, and what major steps take place in the audit process?
 - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
 - How can a plan be designed to study and evaluate internal controls in an application?
 - How can computer audit software be useful in the audit of an application?
 - What is the nature and scope of an operational audit?

INTRODUCTION

- ❖ This session focuses on the concepts and techniques used in auditing an application.
- ❖ Auditors are employed for a wide range of tasks and responsibilities:
 - Organizations employ internal auditors to evaluate company operations.
 - The GAO and state governments employ auditors to evaluate management performance and compliance with legislative intent.
 - The Defense Department employs auditors to review financial records of defense contractors.
 - Publicly-held corporations hire external auditors to provide an independent review of their financial statements.

- ❖ This session is written primarily from the perspective of an internal auditor.
 - They are directly responsible for helping management improve organizational efficiency and effectiveness.
 - They assist in designing and implementing an application that contributes to the entity's goals.
- ❖ External auditors are primarily responsible to shareholders and investors.
 - Only indirectly concerned with application effectiveness.
 - But many internal audit concepts apply to external audits.

❖ Questions to be addressed in this session include:

- **What are the scope and objectives of audit work, and what major steps take place in the audit process?**
- What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
- How can a plan be designed to study and evaluate internal controls in an application?
- How can computer audit software be useful in the audit of an application?
- What is the nature and scope of an operational audit?

Nature of Auditing



THE NATURE OF AUDITING

- ❖ The American Accounting Association (AAA) defines auditing as:
 - 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.
 - Should be carefully planned and techniques should be judiciously selected and executed.
 - Auditing involves collecting, reviewing, and documenting audit evidence.
 - The auditor uses criteria such as the principles of management control discussed in previous sessions to develop recommendations.

THE NATURE OF AUDITING

- ❖ Auditors used to audit around the computer and ignore the computer and programs.
 - Assumption: If output was correctly obtained from system input, then processing must be reliable.
- ❖ Current approach: Audit through the computer.
 - Uses the computer to check adequacy of system controls, data, and output.
 - SAS-94 requires that external auditors evaluate how audit strategy is affected by an organization's use of IT.
 - Also states that auditors may need specialized skills to:
 - Determine how the audit will be affected by IT.
 - Assess and evaluate IT controls.
 - Design and perform both tests of IT controls and substantive tests.

- ❖ Questions to be addressed in this session include:
 - What are the scope and objectives of audit work, and what major steps take place in the audit process?
 - **What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?**
 - How can a plan be designed to study and evaluate internal controls in an application?
 - How can computer audit software be useful in the audit of an application?
 - What is the nature and scope of an operational audit?

❖ Internal Auditing Standards

- According to the IIA, the purpose of an internal audit is to:
 - Evaluate the adequacy and effectiveness of a company's internal control system; and
 - Determine the extent to which assigned responsibilities are carried out.



THE NATURE OF AUDITING

- ❖ The IIA's five audit scope standards outline the internal auditor's responsibilities:
 - Review the reliability and integrity of operating and financial information and how it is identified, measured, classified, and reported.
 - Determine if the systems designed to comply with these policies, plans, procedures, laws, and regulations are being followed.
 - Review how assets are safeguarded, and verify their existence.
 - Examine company resources to determine how effectively and efficiently they are used.
 - Review company operations and programs to determine if they are being carried out as planned and if they are meeting their objectives.

THE NATURE OF AUDITING

- ❖ Today's organizations use a computerized application to process, store, and control company information.
 - To achieve the five preceding objectives, an internal auditor must be qualified to examine all elements of the computerized application and use the computer as a tool to accomplish these auditing objectives.
 - Computer expertise is essential to these tasks.

❖ Types of Internal Auditing Work

- Three different types of audits are commonly performed.
 - **Financial audit**

- ❖ Examines reliability and integrity of accounting records (financial and operating).
- ❖ Correlates with the first of the five scope standards.

THE NATURE OF AUDITING

❖ Types of Internal Auditing Work

- Three different types of audits are commonly performed.
 - Financial audit
 - **Information systems audit**

- ❖ Reviews the controls of an application to assess:
 - Compliance with internal control policies and procedures; and
 - Effectiveness in safeguarding assets.
- ❖ Scope roughly corresponds to the IIA's second and third standards.

THE NATURE OF AUDITING

❖ Types of Internal Auditing Work

- Three different types of audits are commonly performed.
 - Financial audit
 - Information systems audit
 - **Operational or management audit**

- ❖ Concerned with economical and efficient use of resources and accomplishment of established goals and objectives.
- ❖ Scope corresponds to fourth and fifth standards.

THE NATURE OF AUDITING

- ❖ Today's organizations use a computerized application to process, store, and control company information.
 - To achieve the five preceding objectives, an internal auditor must be qualified to examine all elements of the computerized application and use the computer as a tool to accomplish these auditing objectives.
 - Computer expertise is essential to these tasks.

THE NATURE OF AUDITING

Planning

❖ An Overview of the Auditing Process

- All audits follow a similar sequence of activities and may be divided into four stages:
 - **Planning**

THE NATURE OF AUDITING

Planning

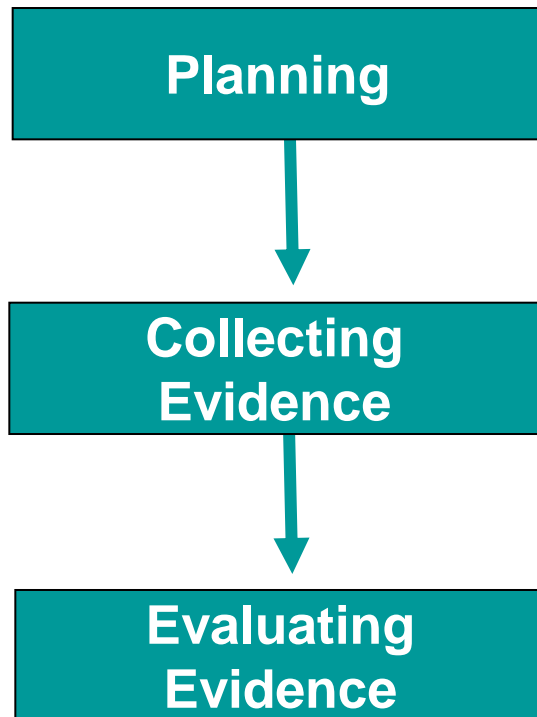


Collecting
Evidence

❖ An Overview of the Auditing Process

- All audits follow a similar sequence of activities and may be divided into four stages:
 - Planning
 - **Collecting Evidence**

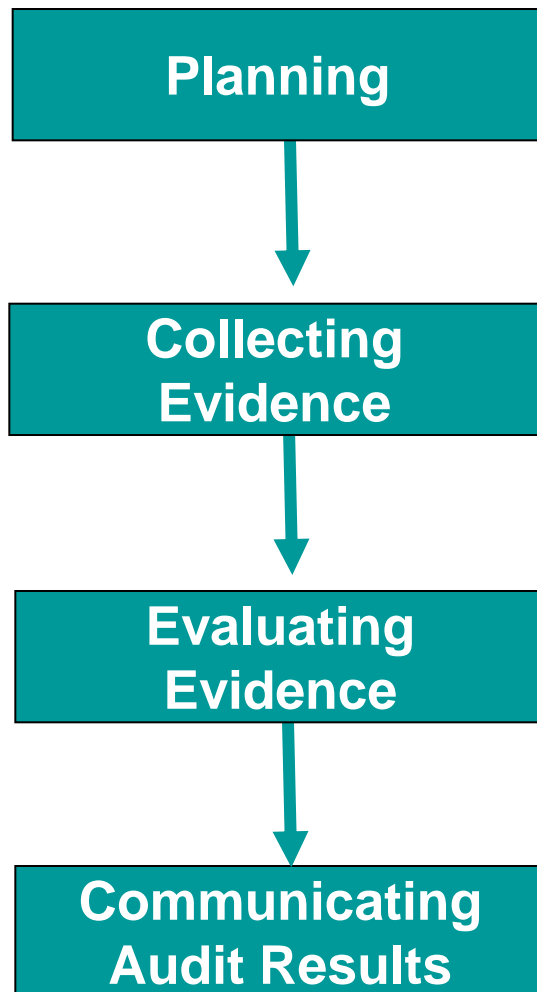
THE NATURE OF AUDITING



❖ An Overview of the Auditing Process

- All audits follow a similar sequence of activities and may be divided into four stages:
 - Planning
 - Collecting evidence
 - **Evaluating evidence**

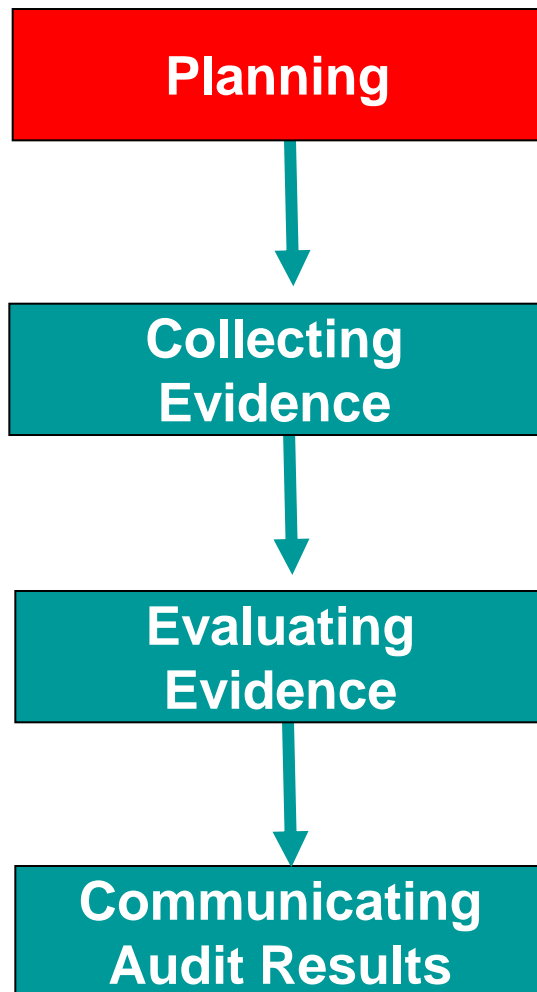
THE NATURE OF AUDITING



❖ An Overview of the Auditing Process

- All audits follow a similar sequence of activities and may be divided into four stages:
 - Planning
 - Collecting evidence
 - Evaluating evidence
 - **Communicating audit results**

THE NATURE OF AUDITING



❖ Audit Planning

- Purpose: Determine why, how, when, and by whom the audit will be performed.
- The first step in audit planning is to establish the scope and objectives of the audit.
- An audit team with the necessary experience and expertise is formed.
- Team members become familiar with the auditee by:
 - Conferring with supervisory and operating personnel;
 - Reviewing system documentation; and
 - Reviewing findings of prior audits.

THE NATURE OF AUDITING

- ❖ The audit should be planned so that the greatest amount of audit work focuses on areas with the highest risk factors.
- ❖ There are three types of risk when conducting an audit:
 - **Inherent risk**
 - How susceptible the area would be to threats if there were no controls.

THE NATURE OF AUDITING

- ❖ The aud... greatest areas wi...
 - ❖ There are... conducting
 - Inherent
 - **Control risk**
- ❖ The risk that a material misstatement will get through the internal control structure and into the financial statements.
 - ❖ Inversely related to the strength of the company's internal controls, i.e., stronger controls means lower control risk.
 - ❖ Can be determined by:
 - Reviewing the control environment.
 - Considering control weaknesses identified in prior audits and evaluating how they have been rectified.

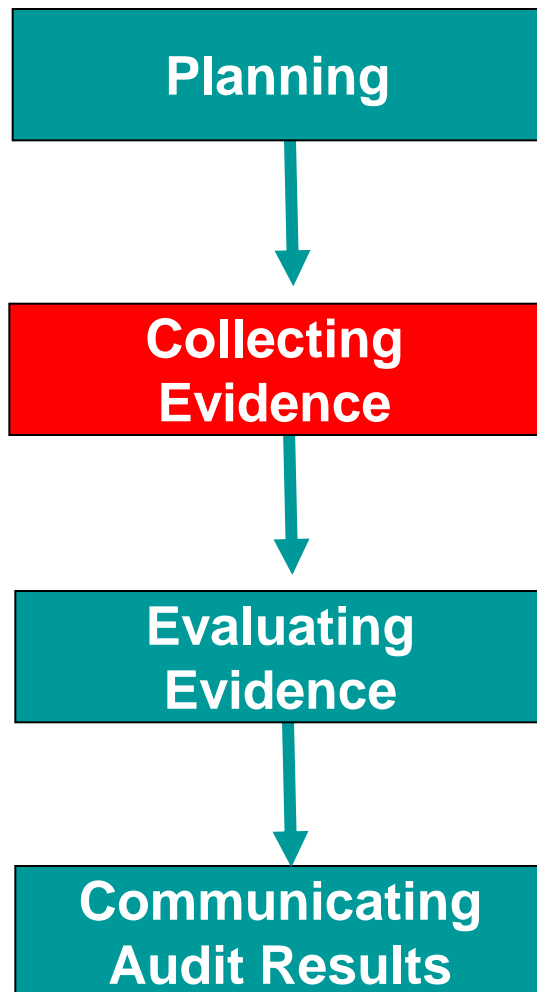
THE NATURE OF AUDITING

- ❖ The audit should be planned so that the greatest amount of audit work focuses on areas with the highest risk factors.
- ❖ There are three types of risk when conducting an audit:
 - Inherent risk
 - Control risk
 - **Detection risk**
 - The risk that auditors and their procedures will miss a material error or misstatement.

THE NATURE OF AUDITING

- ❖ To conclude the planning stage:
 - A preliminary audit program is prepared to show the nature, extent, and timing of the procedures necessary to achieve audit objectives and minimize audit risks.
 - A time budget is prepared.
 - Staff members are assigned to perform specific audit steps.

THE NATURE OF AUDITING



❖ Collection of Audit Evidence

- Much audit effort is spent collecting evidence.

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:

- **Observation**

- Watch the activities being audited, e.g., how employees enter the site or handle a particular form.

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - **Review of documentation**
 - Review documents to understand how an application or an internal control system is supposed to function.

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review of documentation
 - **Discussions**
 - **Talk with employees about their jobs and how they carry out certain procedures.**

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review of documentation
 - Discussions
 - **Physical examination**
 - **Examine quantity and/or condition of tangible assets, such as equipment, inventory, or cash.**

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review of documentation
 - Discussions
 - Physical examination
 - **Confirmation**
 - **Communicate with third parties to check the accuracy of information such as customer account balances.**

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review of documentation
 - Discussions
 - Physical examination
 - Confirmation
 - **Re-performance**
 - Repeat a calculation to verify quantitative information on records and reports.

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review of documentation
 - Discussions
 - Physical examination
 - Conf • **Examine supporting documents to ensure the validity of the transaction.**
 - Re-p
 - **Vouching**

THE NATURE OF AUDITING

❖ Collection of Audit Evidence

- The following are among the most commonly used evidence collection methods:
 - Observation
 - Review
 - ❖ **Examine relationships and trends among information items to detect those that deserve further investigation.**
 - ❖ **Example: If the inventory turnover ratio has plummeted, it's time to investigate why the change has occurred.**
 - Discussion
 - Physical inspection
 - Confirmation
 - Re-performance
 - Voluntary disclosure
 - Analytical review

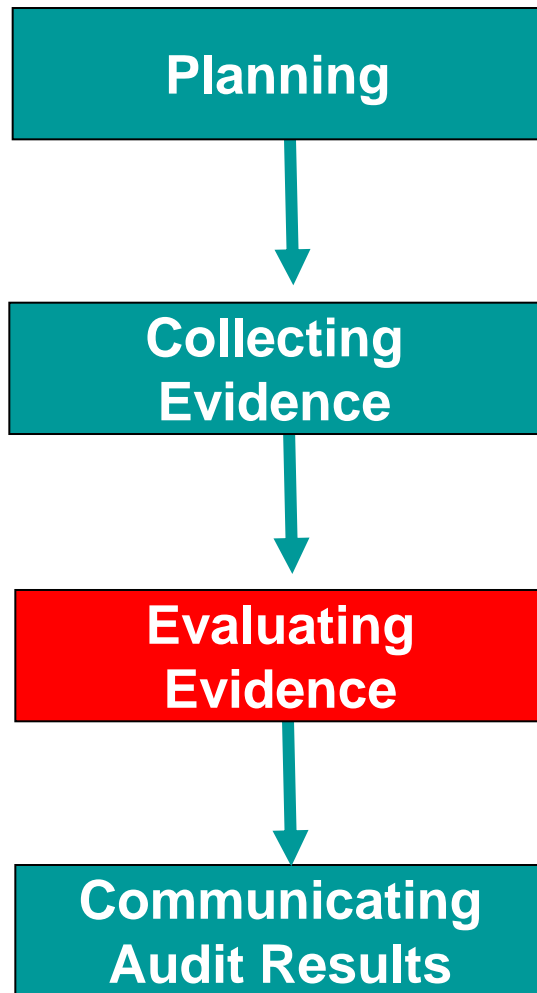


THE NATURE OF AUDITING

- ❖ Because many audit tests and procedures cannot feasibly be performed on the entire set of activities, records, assets, or documents, they are often performed on a sample basis.
- ❖ A typical audit will be a mix of audit procedures.

THE NATURE OF AUDITING

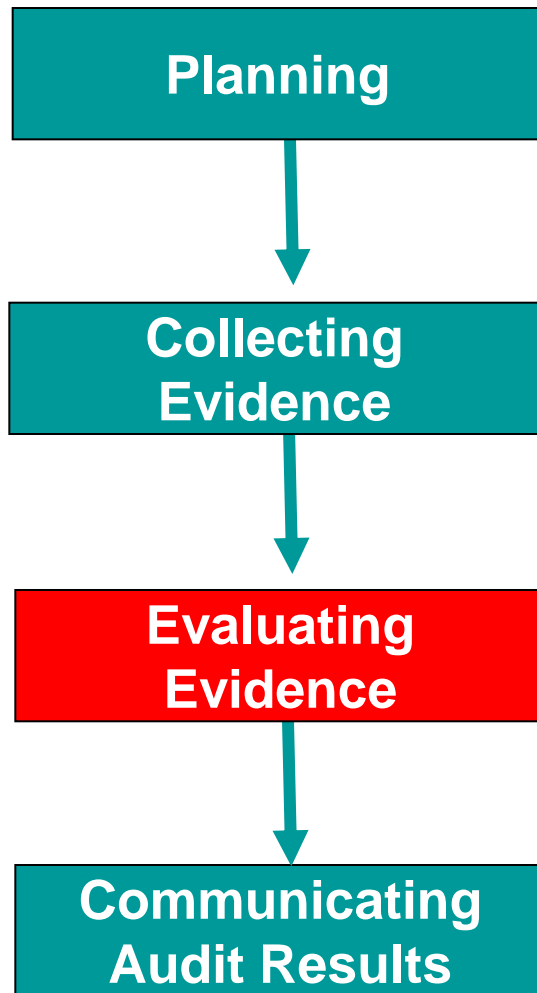
- ❖ An audit designed to evaluate application internal controls would make greater use of:
 - Observation
 - Review of documentation
 - Discussions
 - Re-performance
- ❖ An audit of financial information would focus on:
 - Physical examination
 - Confirmation
 - Vouching
 - Analytical review
 - Re-performance



- ❖ Because errors will occur anywhere, auditors focus on those that have a significant impact on management's interpretation of the audit findings.
- ❖ Materiality dictates what is and is not important in a given set of circumstances—primarily a matter of judgment.
- ❖ It is generally more important to external audits, when the overall emphasis is on the fairness of financial statement presentations, than to internal audits, where the focus is on determining adherence to management's policies.

- **Materiality**

THE NATURE OF AUDITING



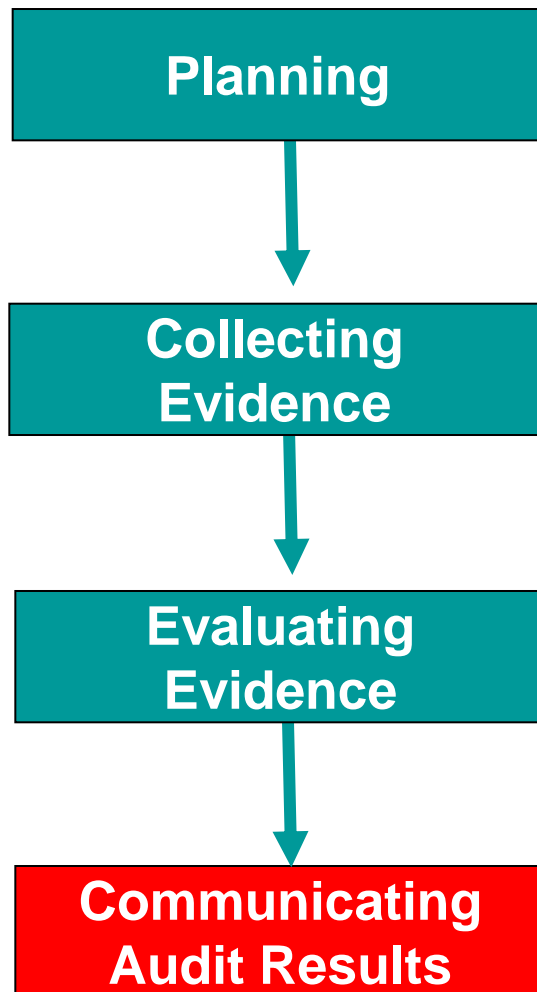
- ❖ Reasonable assurance is somewhat of a cost-benefit notion.
- ❖ It is prohibitively expensive for the auditor to seek complete assurance that no material error exists, so he must accept risk that the audit conclusion is incorrect.
- ❖ Therefore he seeks reasonable assurance, as opposed to absolute assurance.
- ❖ Note that when inherent or control risk is high, the auditor must obtain greater assurance to offset the greater uncertainty and risks.

- **Reasonable assurance**

THE NATURE OF AUDITING

- ❖ At all stages of the audit, findings and conclusions are carefully documented in working papers.
- ❖ Documentation is critical at the evaluation stage, when final conclusions must be reached and supported.

THE NATURE OF AUDITING



❖ Communication of audit results

- The auditor prepares a written (and sometimes oral) report summarizing audit findings and recommendations, with references to supporting evidence in the working papers.
- Report is presented to:
 - Management
 - The audit committee
 - The board of directors
 - Other appropriate parties
- After results are communicated, auditors often perform a follow-up study to see if recommendations have been implemented.

THE NATURE OF AUDITING

❖ *The Risk-Based Audit Approach*

- A risk-based audit approach is a four-step approach to internal control evaluation that provides a logical framework for carrying out an audit. Steps are:
 - **Determine the threats (errors and irregularities) facing the application.**

THE NATURE OF AUDITING

❖ *The Risk-Based Audit Approach*

- A risk-based audit approach is a four-step approach to internal control evaluation that provides a logical framework for carrying out an audit. Steps are:
 - Determine the threats (errors and irregularities) facing the application.
 - **Identify control procedures implemented to minimize each threat by preventing or detecting such errors and irregularities.**

THE NATURE OF AUDITING

❖ **The Risk**

- A risk-
to inter
framev
- Dete
appl
- Ident
threa
irreg

- ❖ Perform a *systems review* to determine if necessary procedures are in place. Involves:
 - Reviewing system documentation
 - Interviewing appropriate personnel
- ❖ Conduct *tests of controls* to determine if the procedures are satisfactorily followed. Involves:
 - Observing system operations
 - Inspecting documents, records, and reports
 - Checking samples of system inputs and outputs
 - Tracing transactions through the system

- **Evaluate the control procedures.**

THE NATURE OF AUDITING

❖ *The Risk-Based Audit Approach*

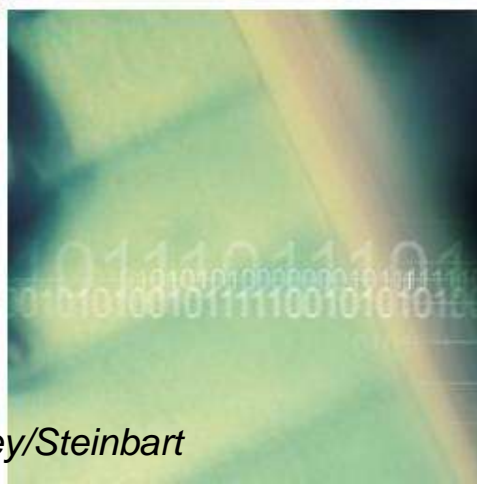
- A risk-based approach to internal control framework
 - Determine the risk of material misstatement
 - Identify and assess the risks of material misstatement
 - Evaluate the design and implementation of internal control
 - Evaluate weaknesses (errors and irregularities not covered by control procedures) to determine their effect on the nature, timing, or extent of auditing procedures and client suggestions.
- ❖ Focuses on control risks and whether the control system as a whole adequately addresses them.
- ❖ If a control deficiency is identified, the auditor asks about *compensating controls*—procedures that make up for the deficiency.
- ❖ A control weakness in one area may be acceptable if compensated for by control strengths in other areas.



THE NATURE OF AUDITING

- ❖ 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 basis for developing recommendations to management on how the application control system should be improved.

Information Systems Audit



- ❖ Questions to be addressed in this session include:
 - What are the scope and objectives of audit work, and what major steps take place in the audit process?
 - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
 - **How can a plan be designed to study and evaluate internal controls in an application?**
 - How can computer audit software be useful in the audit of an application?
 - What is the nature and scope of an operational audit?

INFORMATION SYSTEMS AUDITS

- ❖ The purpose of an information systems audit is to review and evaluate the internal controls that protect the system.
- ❖ When performing an information system audit, auditors should ascertain that the following objectives are met:
 - Security provisions protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.
 - Program development and acquisition are performed in accordance with management's general and specific authorization.
 - Program modifications have management's authorization and approval.

INFORMATION SYSTEMS AUDITS

- Processing of transactions, files, reports, and other computer records is accurate and complete.
 - Source data that are inaccurate or improperly authorized are identified and handled according to prescribed managerial policies.
 - Computer data files are accurate, complete, and confidential.
- ❖ The following slide depicts the relationship among these six objectives and information systems components.
 - ❖ The objectives are then discussed in detail in the following section.
 - ❖ Each description includes an audit plan to accomplish the objective, as well as the techniques and procedures to carry out the plan.

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

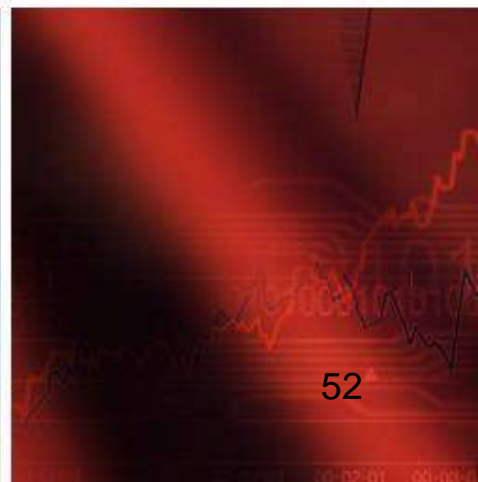
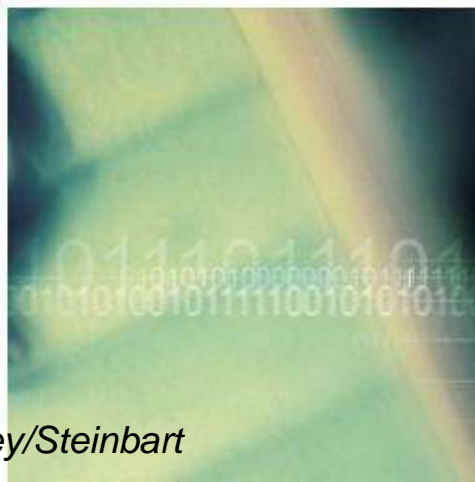
Objective 3:
Program Modification

Objective 4: Computer Processing

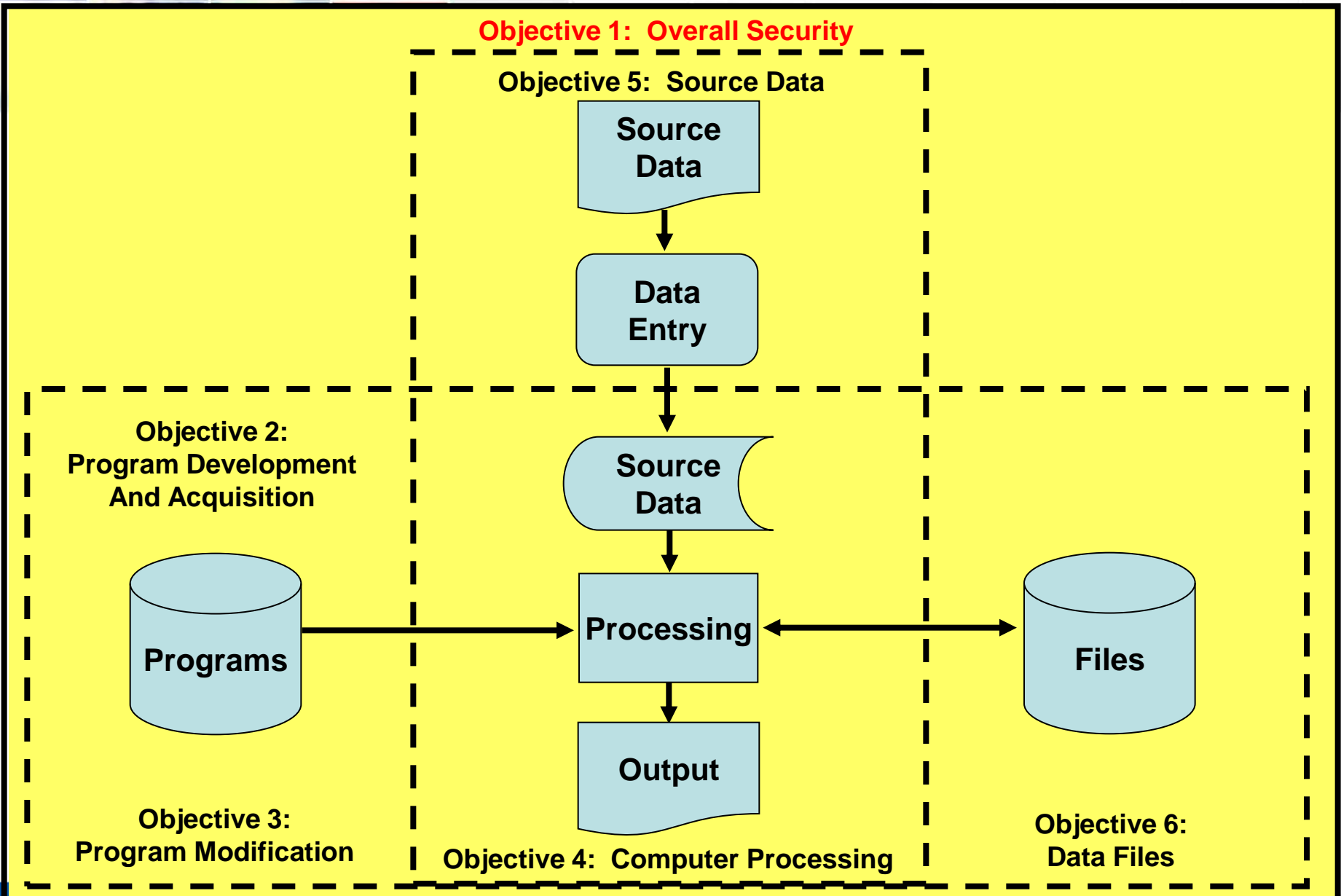
Files

Objective 6:
Data Files

Objective 1: Overall Security



IS COMPONENTS AND AUDIT OBJECTIVES



OBJECTIVE 1: OVERALL SECURITY

- ❖ **Types of security errors and fraud faced by companies:**
 - Accidental or intentional damage to system assets.
 - Unauthorized access, disclosure, or modification of data and programs.
 - Theft.
 - Interruption of crucial business activities.

OBJECTIVE 1: OVERALL SECURITY

❖ Control procedures to minimize security errors and fraud:

- Developing an information security/protection plan.
- Restricting physical and logical access.
- Encrypting data.
- Protecting against viruses.
- Implementing firewalls.
- Instituting data transmission controls.
- Preventing and recovering from system failures or disasters, including:
 - Designing fault-tolerant systems.
 - Preventive maintenance.
 - Backup and recovery procedures.
 - Disaster recovery plans.
 - Adequate insurance.



OBJECTIVE 1: OVERALL SECURITY

❖ Audit Procedures: Systems Review

- Inspecting computer sites.
- Interviewing personnel.
- Reviewing policies and procedures.
- Examining access logs, insurance policies, and the disaster recovery plan.

❖ Audit Procedures: Tests of Controls

- Auditors test security controls by:
 - Observing procedures.
 - Verifying that controls are in place and work as intended.
 - Investigating errors or problems to ensure they were handled correctly.
 - Examining any tests previously performed.
- One way to test logical access controls is to try to break into a system.

OBJECTIVE 1: OVERALL SECURITY

❖ **Compensating Controls**

- If security controls are seriously deficient, the organization faces substantial risks.
- Partial compensation for poor computer security can be provided by:
 - Sound personnel policies
 - Effective segregation of incompatible duties
 - Effective user controls, so that users can recognize unusual system output.
- These compensations aren't likely to be enough, so auditors should strongly recommend that security weaknesses be corrected.

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

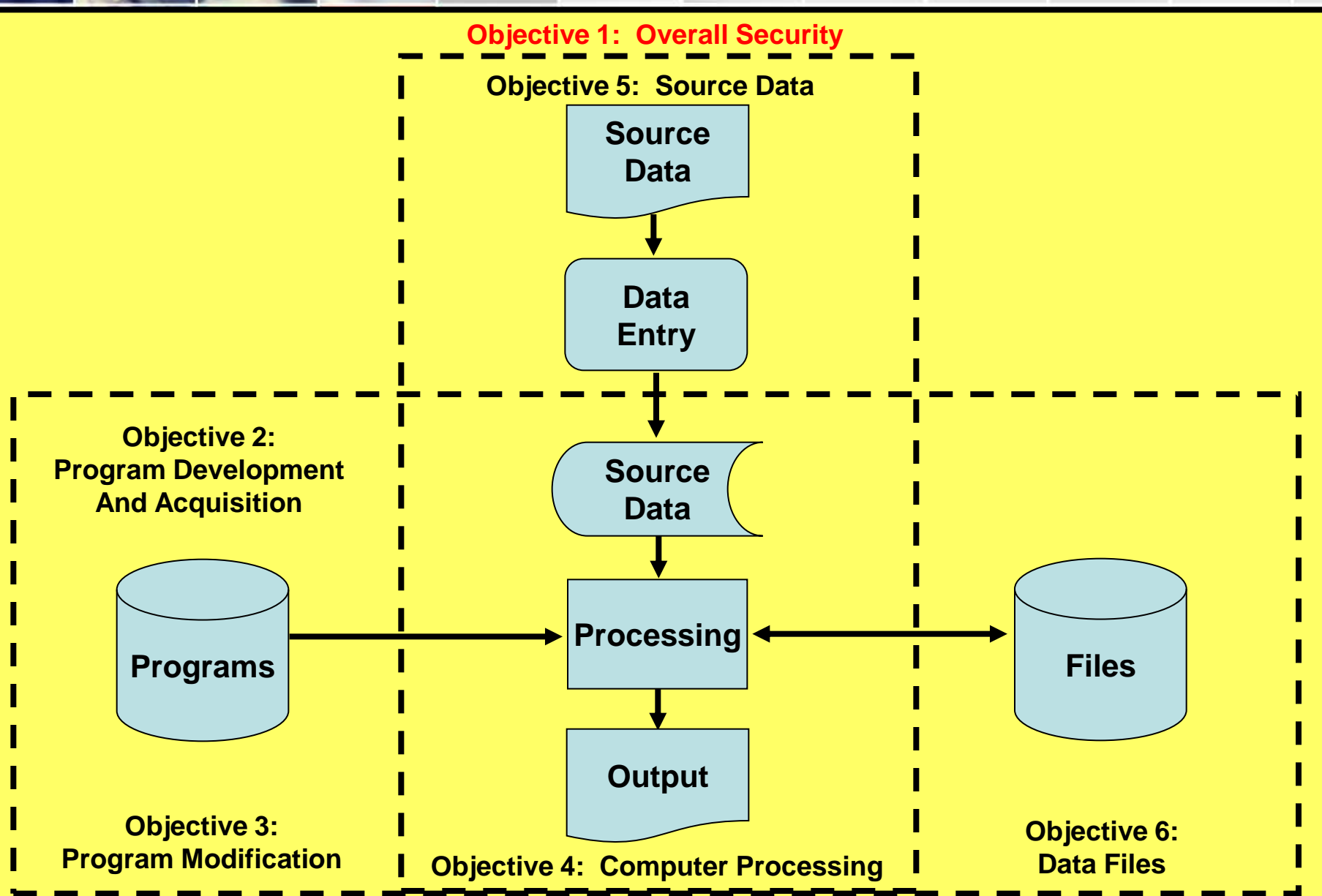
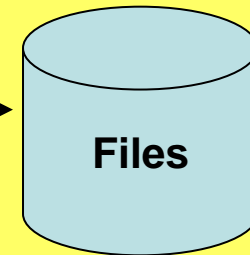
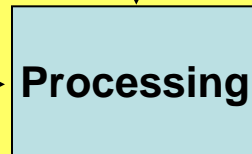
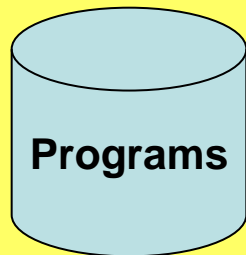
Objective 2: Program Development And Acquisition

Programs

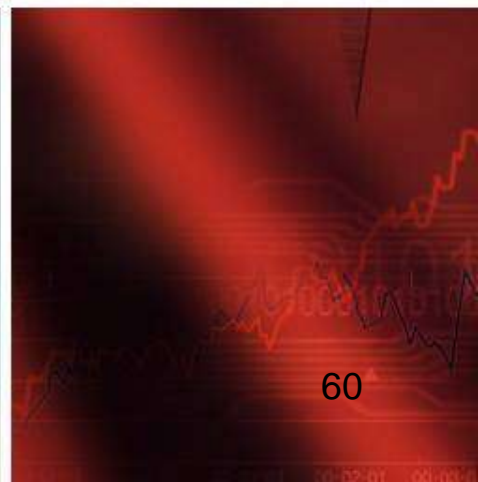
Objective 3: Program Modification

Objective 4: Computer Processing

Objective 6: Data Files



Objective 2: Program Development & Acquisition



IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

Objective 3:
Program Modification

Files

Objective 6:
Data Files

Objective 4: Computer Processing



OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

❖ **Types of errors and fraud:**

- Two things can go wrong in program development:
 - Inadvertent errors due to careless programming or misunderstanding specifications; or
 - Deliberate insertion of unauthorized instructions into the programs.



OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

❖ Control procedures:

- The preceding problems can be controlled by requiring:
 - Management and user authorization and approval
 - Thorough testing
 - Proper documentation



OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

❖ Audit Procedures: Systems Review

- The auditor's role in systems development should be limited to an independent review of system development activities.
 - To maintain necessary objectivity for performing an independent evaluation, the auditor should not be involved in system development.
 - During the systems review, the auditor should gain an understanding of development procedures by discussing them with management, users, and IS personnel.
 - Should also review policies, procedures, standards, and documentation for systems and programs.



OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

❖ Audit Procedures: Tests of Controls

- To test systems development controls, auditors should:
 - Interview managers and system users.
 - Examine development approvals.
 - Review the minutes of development team meetings.
 - Thoroughly review all documentation relating to the testing process and ascertain that all program changes were tested.
 - Examine the test specifications, review the test data, and evaluate the test results.
 - If results were unexpected, ascertain how the problem was resolved.



OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

❖ **Compensating Controls**

- Strong processing controls can sometimes compensate for inadequate development controls.
 - If auditors rely on compensatory processing controls, they should obtain persuasive evidence of compliance.
 - Use techniques such as independent processing of test data to do so.
 - If this type of evidence can't be obtained, they may have to conclude there is a material weakness in internal control.

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

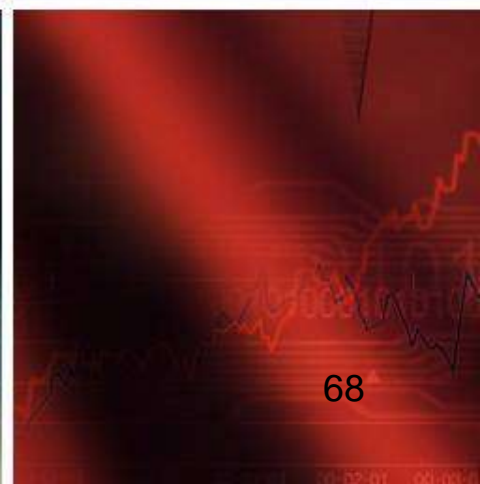
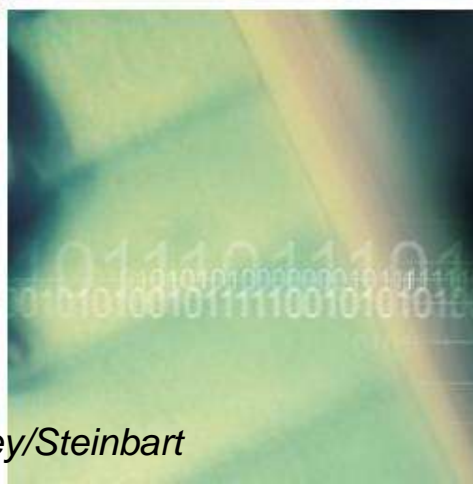
Objective 3:
Program Modification

Files

Objective 6:
Data Files

Objective 4: Computer Processing

Objective 3: Program Modification



IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

Objective 3:
Program Modification

Files

Objective 6:
Data Files

Objective 4: Computer Processing

❖ Types of Errors and Fraud

- Same that can occur during program development:
 - Inadvertent programming errors
 - Unauthorized programming code

OBJECTIVE 3: PROGRAM MODIFICATION

❖ Control Procedures

- When a program change is submitted for approval, a list of all required updates should be compiled by management and program users.
- Changes should be thoroughly tested and documented.
- During the change process, the developmental version of the program must be kept separate from the production version.
- When the amended program has received final approval, it should replace the production version.
- Changes should be implemented by personnel independent of users or programmers.
- Logical access controls should be employed at all times.

OBJECTIVE 3: PROGRAM MODIFICATION


❖ Audit Procedures: System Review

- During systems review, auditors should:
 - Gain an understanding of the change process by discussing it with management and user personnel.
 - Examine the policies, procedures, and standards for approving, modifying, testing, and documenting the changes.
 - Review a complete set of final documentation materials for recent program changes, including test procedures and results.
 - Review the procedures used to restrict logical access to the developmental version of the program.

OBJECTIVE 3: PROGRAM MODIFICATION

❖ Audit Procedures: Tests of Controls

- An important part of these tests is to verify that program changes were identified, listed, approved, tested, and documented.
- Requires that the auditor observe how changes are implemented to verify that:
 - Separate development and production programs are maintained; and
 - Changes are implemented by someone independent of the user and programming functions.
- The auditor should review the development program's access control table to verify that only those users assigned to carry out modification had access to the system.



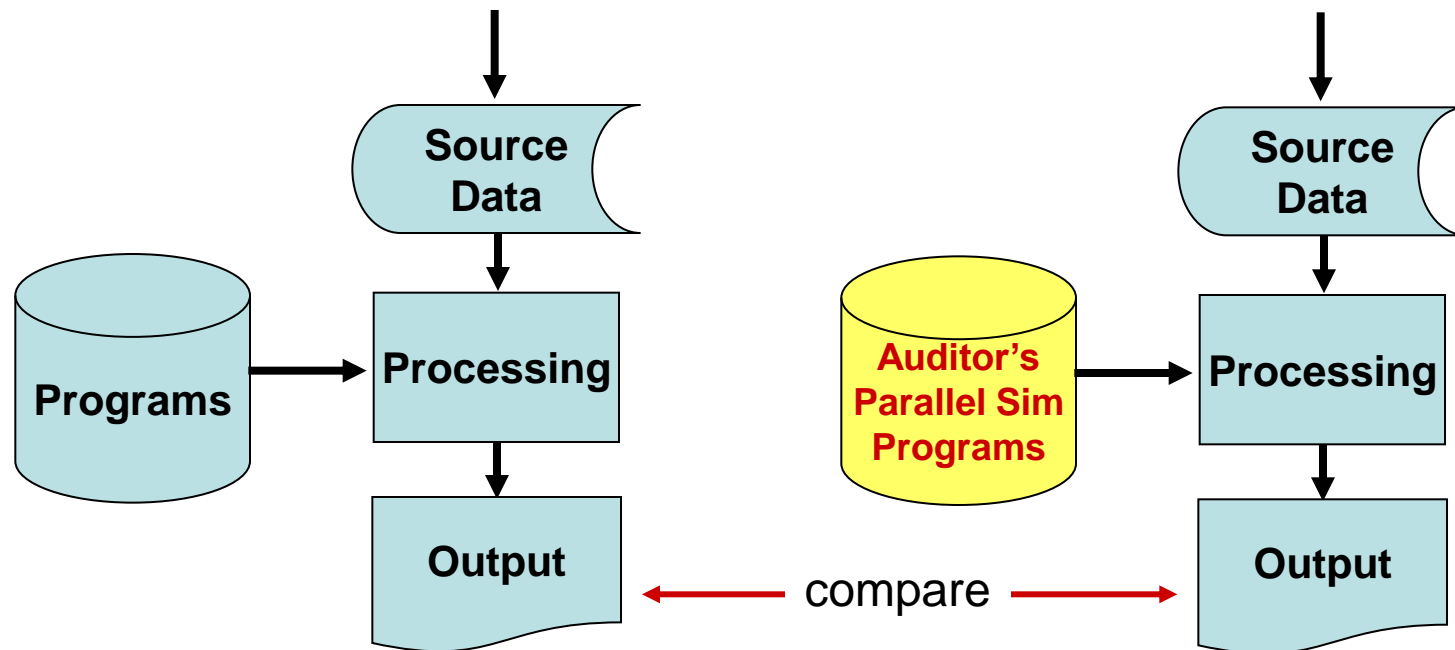
OBJECTIVE 3: PROGRAM MODIFICATION


- To test for unauthorized program changes, auditors can use a source code comparison program to compare the current version of the program with the original source code.
 - Any unauthorized differences should result in an investigation.
 - If the difference represents an authorized change, the auditor can refer to the program change specifications to ensure that the changes were authorized and correctly incorporated.

OBJECTIVE 3: PROGRAM MODIFICATION

- Two additional techniques detect unauthorized program changes:
 - Reprocessing
 - On a surprise basis, the auditor uses a verified copy of the source code to reprocess data and compare that output with the company's data.
 - Discrepancies are investigated.
 - Parallel simulation
 - Similar to reprocessing except that the auditor writes his own program instead of using verified source code.
 - Can be used to test a program during the implementation process.

Parallel Simulation





OBJECTIVE 3: PROGRAM MODIFICATION

- Auditors should observe testing and implementation, review related authorizations, and, if necessary, perform independent tests for each major program change.
- If this step is skipped and program change controls are subsequently deemed inadequate, it may not be possible to rely on program outputs.
- Auditors should always test programs on a surprise basis to protect against unauthorized changes being inserted after the examination is completed and then removed prior to scheduled audits.

OBJECTIVE 3: PROGRAM MODIFICATION

❖ **Compensating Controls**

- If internal controls over program changes are deficient, compensation controls are:
 - Source code comparison;
 - Reprocessing; and/or
 - Parallel simulation.
- The presence of sound processing controls, independently tested by the auditor, can also partially compensate for deficiencies.
- But if deficiencies are caused by inadequate restrictions on program file access, the auditor should strongly recommend actions to strengthen the organization's logical access controls.

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

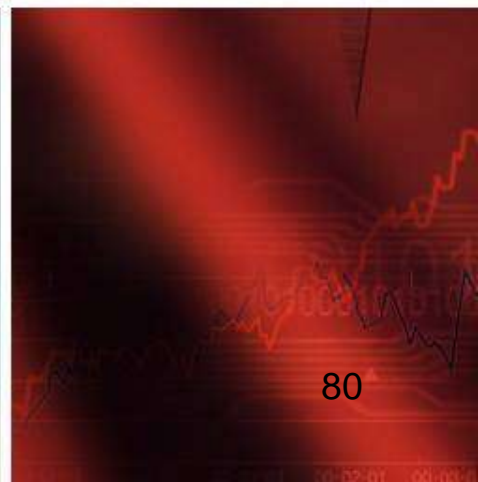
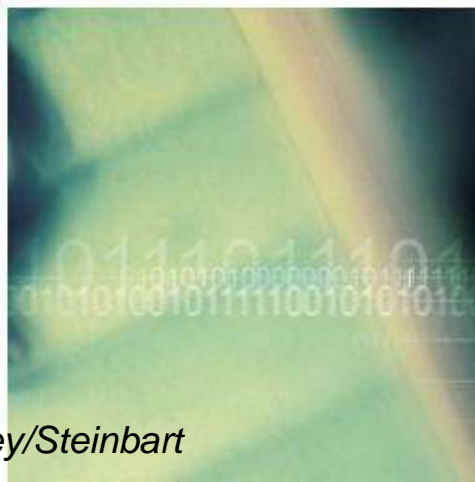
Objective 3:
Program Modification

Files

Objective 6:
Data Files

Objective 4: Computer Processing

Objective 4: Computer Processing



IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

Objective 3:
Program Modification

Files

Objective 6:
Data Files

Objective 4: Computer Processing

❖ Types of Errors and Fraud

- During computer processing, the system may:
 - Fail to detect erroneous input
 - Improperly correct input errors
 - Process erroneous input
 - Improperly distribute or disclose output

OBJECTIVE 4: COMPUTER PROCESSING

❖ 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

OBJECTIVE 4: COMPUTER PROCESSING

❖ Audit Procedures: Systems 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 and output controls with operations and IS supervisory personnel

OBJECTIVE 4: COMPUTER PROCESSING

❖ 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

OBJECTIVE 4: COMPUTER PROCESSING

- 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 online processing systems using concurrent audit techniques
- Recreate selected reports to test for accuracy and completeness

❖ **Compensating Controls**

- Auditors must periodically reevaluate processing controls to ensure their continued reliability.
 - If controls are unsatisfactory, user and source data controls may be strong enough to compensate.
 - If not, a material weakness exists and steps should be taken to eliminate the control deficiencies.

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The purpose of the preceding audit procedures is to gain an understanding of the controls, evaluate their adequacy, and observe operations for evidence that the controls are in use.
- ❖ Several specialized techniques allow the auditor to use the computer to test processing controls:
 - Processing test data
 - Using concurrent audit techniques
 - Analyzing program logic
- ❖ Each has its own advantages and disadvantages:
 - Appropriateness of each technique depends on the situation
 - No one technique is good for all circumstances
- ❖ Auditors should not disclose which technique they use.


OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The purpose of the preceding audit procedures is to gain an understanding of the controls, evaluate their adequacy, and observe operations for evidence that the controls are in use.
- ❖ Several specialized techniques allow the auditor to use the computer to test processing controls:
 - **Processing test data**
 - Using concurrent audit techniques
 - Analyzing program logic
- ❖ Each has its own advantages and disadvantages:
 - Appropriateness of each technique depends on the situation
 - No one technique is good for all circumstances
- ❖ Auditors should not disclose which technique they use.

OBJECTIVE 4: COMPUTER PROCESSING


❖ Processing Test Data

- Involves testing a program by processing a hypothetical series of valid and invalid transactions.
- The program should:
 - Process all the valid transactions correctly.
 - Identify and reject the invalid ones.
- All logic paths should be checked for proper functioning by one or more test transactions, including:
 - Records with missing data
 - Fields containing unreasonably large amounts
 - Invalid account numbers or processing codes
 - Non-numeric data in numeric fields
 - Records out of sequence



OBJECTIVE 4: COMPUTER PROCESSING

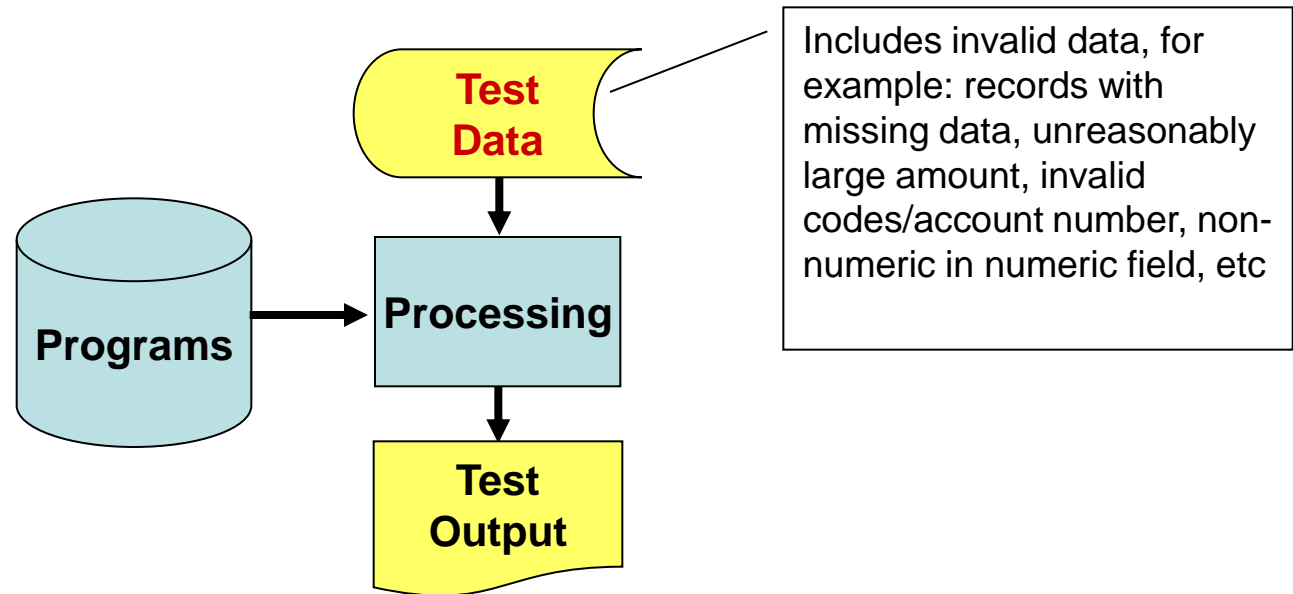
- ❖ The following resources are helpful when preparing test data:
 - A listing of actual transactions
 - The transactions that the programmer used to test the program
 - A ***test data generator program***, which automatically prepares test data based on program specifications




OBJECTIVE 4: COMPUTER PROCESSING

- ❖ In a batch processing system, the company's program and a copy of relevant files are used to process the test data.
 - Results are compared with the predetermined correct output.
 - Discrepancies indicate processing errors or control deficiencies that should be investigated.
- ❖ In an online system, auditors enter test data using a data entry device, such as a PC or terminal.
 - The auditor observes and logs the system's response.
 - If the system accepts erroneous or invalid test transactions, the auditor reverses the effects of the transactions, investigates the problem, and corrects the deficiency.

Processing Test Data





OBJECTIVE 4: COMPUTER PROCESSING

- ❖ Although processing test transactions is usually effective, it has the following disadvantages:
 - The auditor must spend considerable time understanding the system and preparing an adequate set of test transactions.
 - Care must be taken to ensure test data do not affect the company's files and databases.
 - The auditor can reverse the effects of the test transactions or process them in a separate run, using a copy of the file or database.
 - Reversal procedures may reveal the existence and nature of the auditor's test to key personnel.
 - A separate run removes some of the authenticity.

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The purpose of the preceding audit procedures is to gain an understanding of the controls, evaluate their adequacy, and observe operations for evidence that the controls are in use.
- ❖ Several specialized techniques allow the auditor to use the computer to test processing controls:
 - Processing test data
 - **Using concurrent audit techniques**
 - Analyzing program logic
- ❖ Each has its own advantages and disadvantages:
 - Appropriateness of each technique depends on the situation
 - No one technique is good for all circumstances
- ❖ Auditors should not disclose which technique they use.

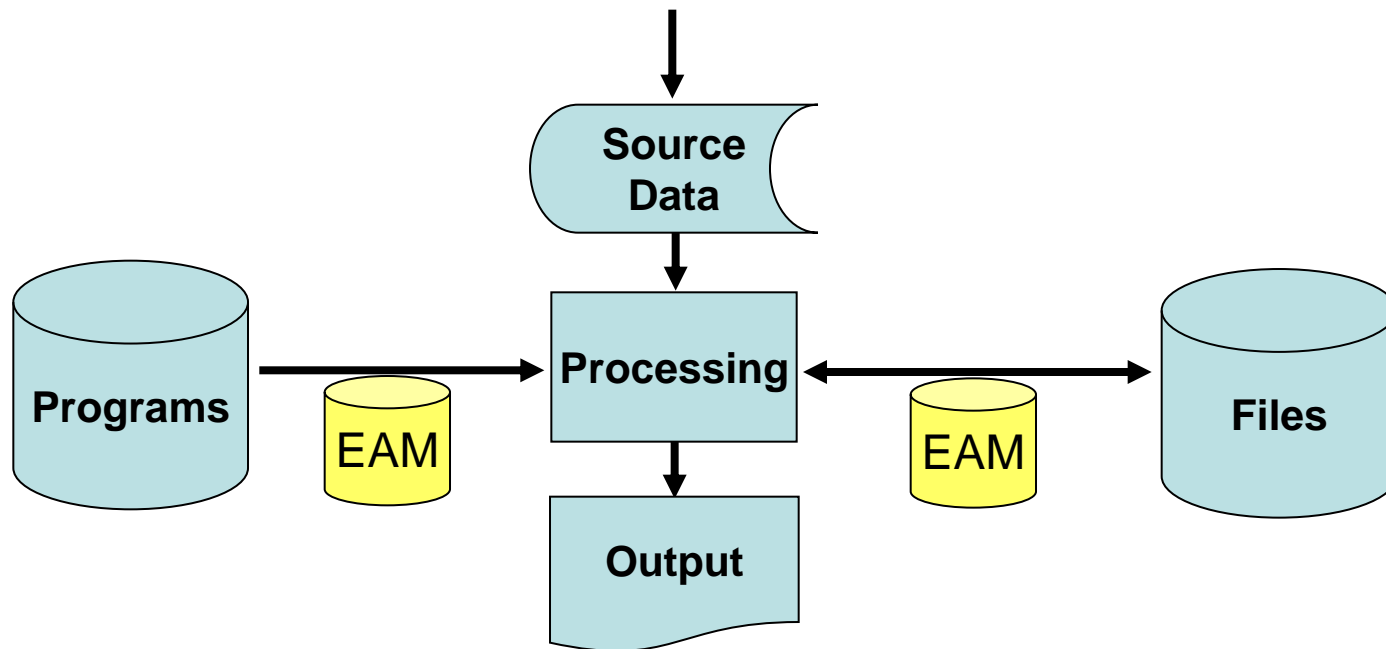
OBJECTIVE 4: COMPUTER PROCESSING

❖ Concurrent audit techniques

- Millions of dollars of transactions can be processed in an online system without leaving a satisfactory audit trail.
- In such cases, evidence gathered after data processing is insufficient for audit purposes.
- Also, because many online systems process transactions continuously, it is difficult or impossible to stop the system to perform audit tests.
- Consequently, auditors use **concurrent audit techniques** to continually monitor the system and collect audit evidence while live data are processed during regular operating hours.

- ❖ **Concurrent audit techniques use *embedded audit modules*.**
 - These are segments of program code that:
 - Perform audit functions;
 - Report test results to the auditor; and
 - Store collected evidence for auditor review.
 - Are time-consuming and difficult to use, but less so if incorporated when programs are developed.

Embedded Audit Module



❖ Auditors commonly use five concurrent audit techniques:

- An integrated test facility (ITF) technique
- A snapshot technique
- A system control audit review file (SCARF)
- Audit hooks
- Continuous and intermittent simulation (CIS)

❖ Auditors commonly use five concurrent audit techniques:

- **An integrated test facility (ITF) technique**
- A snapshot technique
- A system control audit review file (SCARF)
- Audit hooks
- Continuous and intermittent simulation (CIS)

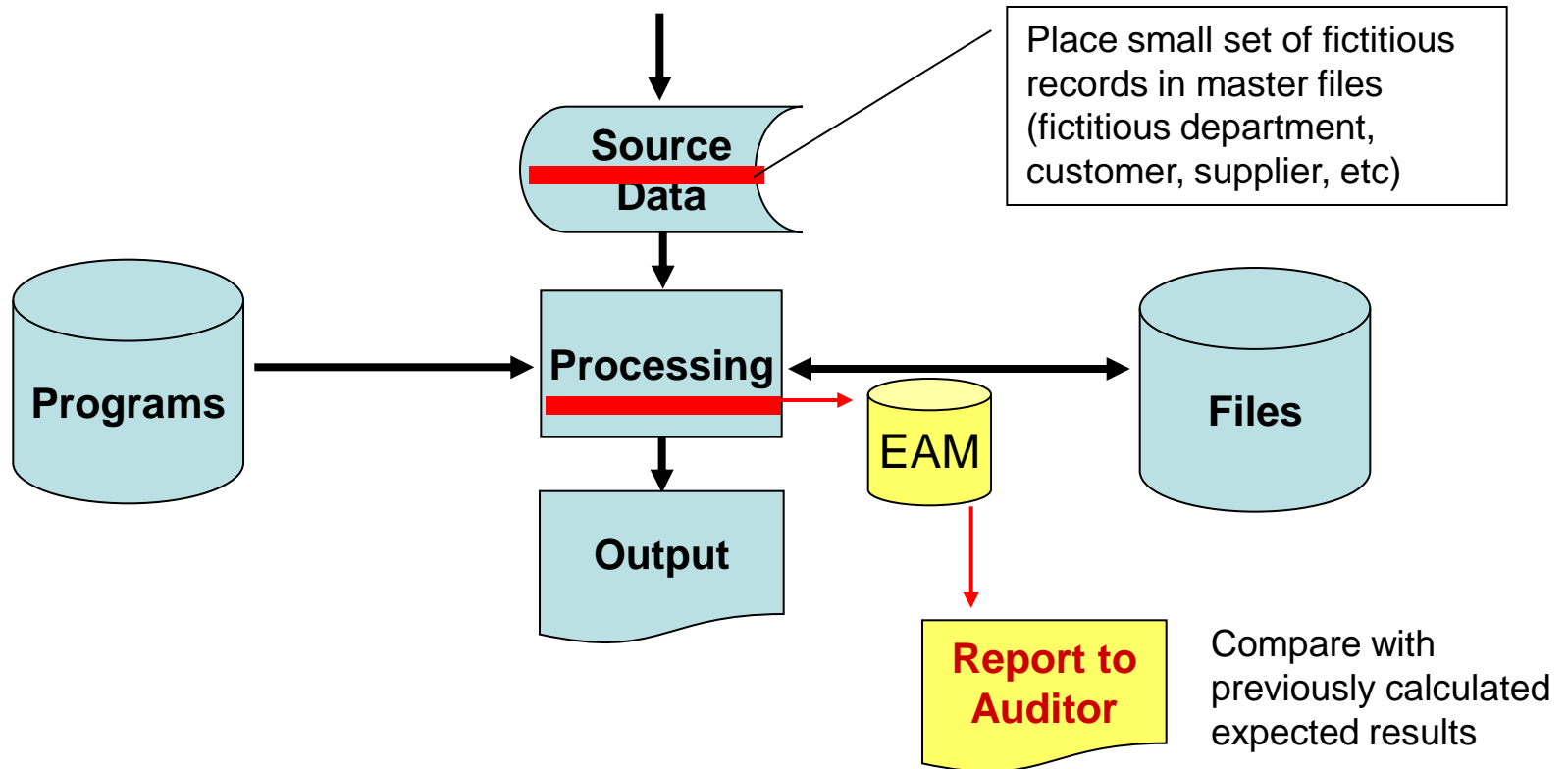
OBJECTIVE 4: COMPUTER PROCESSING

- ❖ An ***ITF technique*** places a small set of fictitious records in the master files:
 - May represent a fictitious division, department, office, customer, or supplier.
 - Processing test transactions to update these dummy records will not affect actual records.
 - Because real and fictitious transactions are processed together, company employees don't know the testing is taking place.

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The system must:
 - Distinguish ITF from actual records;
 - Collect information on the effects of test transactions;
 - Report the results.
- ❖ The auditor compares processing with expected results to verify system and controls are operating correctly.

Integrated Test Facility




OBJECTIVE 4: COMPUTER PROCESSING

- ❖ In a batch processing system, the ITF technique
 - Eliminates the need to reverse test transactions
 - Is easily concealed from operating employees because test transactions don't need to be reversed.
- ❖ In online processing systems, test transactions can be:
 - Submitted on a frequent basis
 - Processed with actual transactions
 - Traced through every processing stage
- ❖ Can all be accomplished without disrupting regular processing operations.
- ❖ Care must be taken not to include dummy records in the reporting process.

❖ Auditors commonly use five concurrent audit techniques:

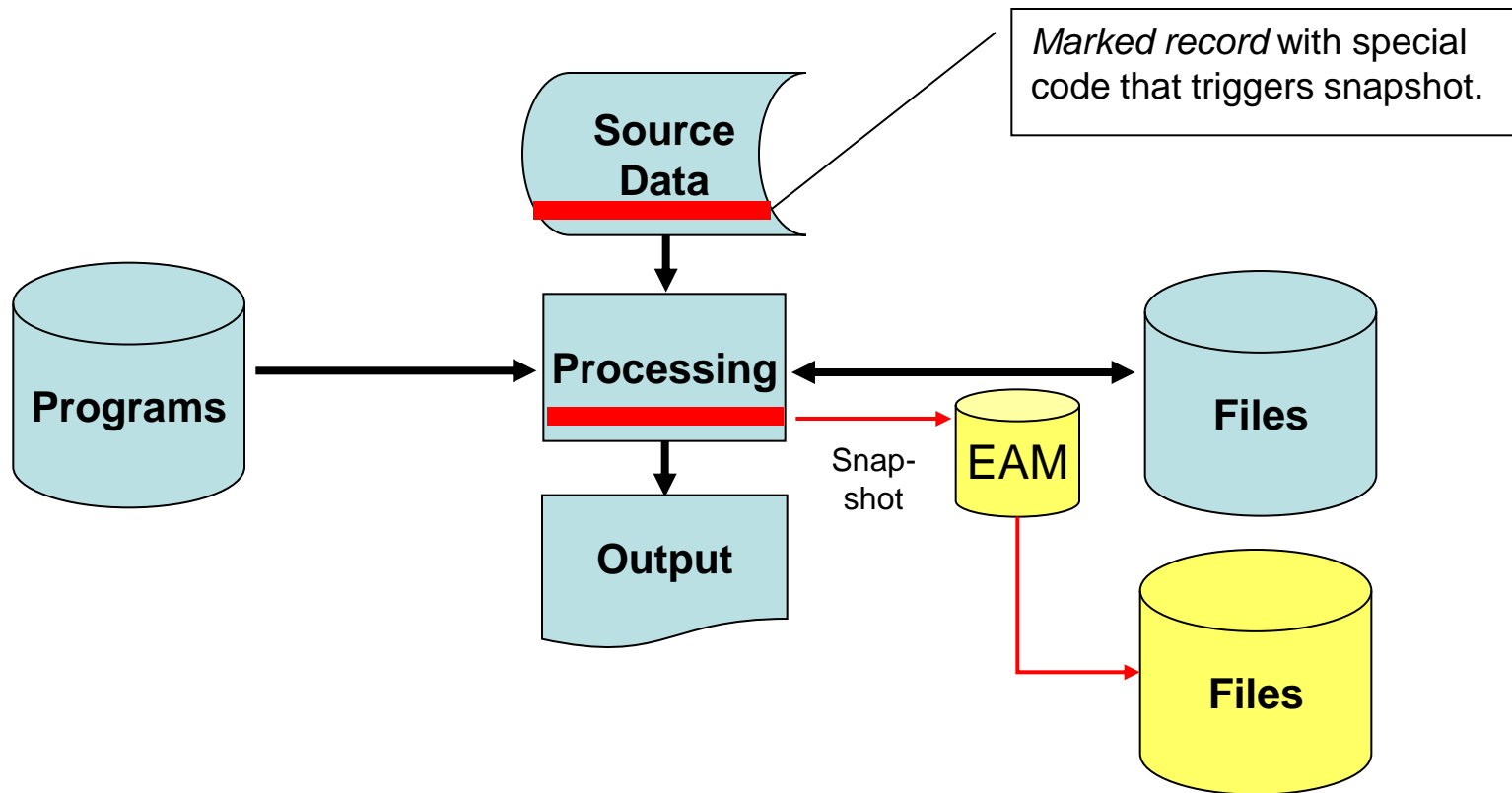
- An integrated test facility (ITF) technique
- **A snapshot technique**
- A system control audit review file (SCARF)
- Audit hooks
- Continuous and intermittent simulation (CIS)



OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The ***snapshot technique*** examines the way transactions are processed.
 - Selected transactions are marked with a special code that triggers the snapshot process.
 - Audit modules in the program record these transactions and their master file records before and after processing.
 - The selected data are recorded in a special file and reviewed by the auditor to verify that all processing steps were properly executed.

Snapshot Technique



Reviewed by auditors to verify that all processing steps have been executed

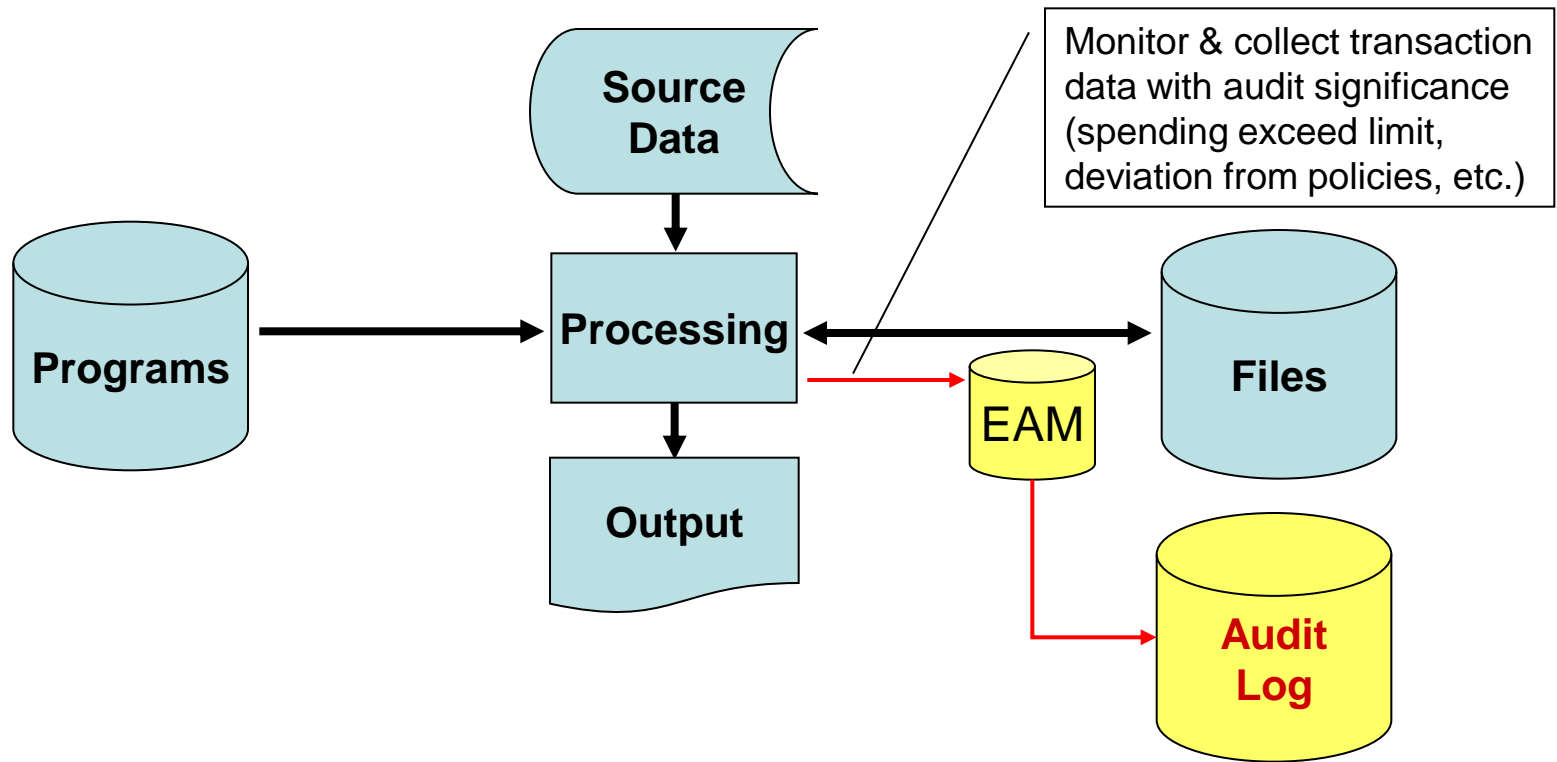
❖ Auditors commonly use five concurrent audit techniques:

- An integrated test facility (ITF) technique
- A snapshot technique
- **A system control audit review file (SCARF)**
- Audit hooks
- Continuous and intermittent simulation (CIS)

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ The ***system control audit review file (SCARF)*** uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance.
- ❖ Data recorded in a SCARF file or *audit log* include transactions that:
 - Exceed a specified dollar limit;
 - Involve inactive accounts;
 - Deviate from company policy; or
 - Contain write-downs of asset values.
- ❖ Periodically the auditor:
 - Receives a printout of SCARF transactions;
 - Looks for questionable transactions among them; and
 - Investigates.

Systems Control Audit Review File (SCARF)



Auditor reviews log for follow-ups

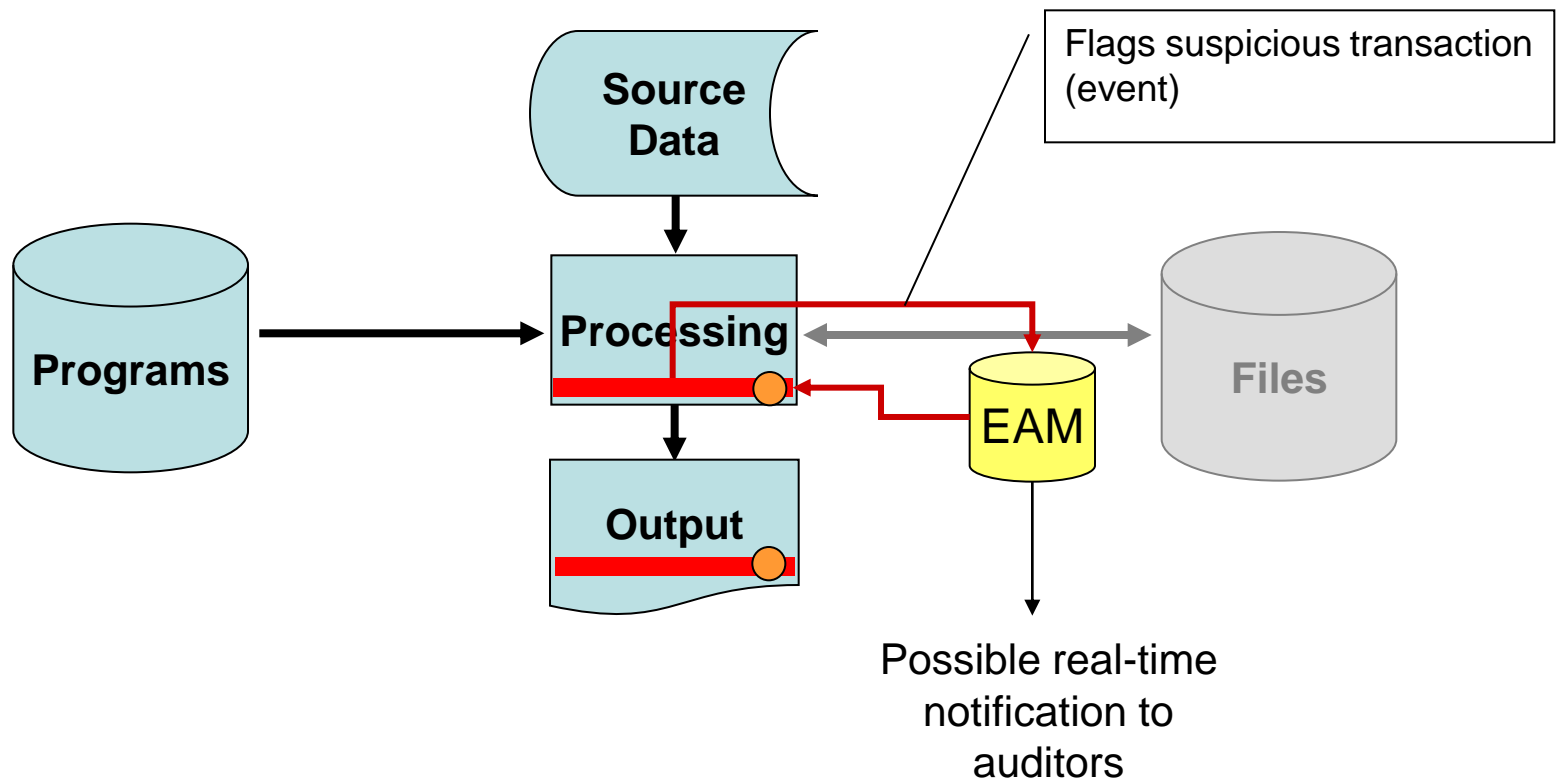
❖ Auditors commonly use five concurrent audit techniques:

- An integrated test facility (ITF) technique
- A snapshot technique
- A system control audit review file (SCARF)
- **Audit hooks**
- Continuous and intermittent simulation (CIS)

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ ***Audit hooks*** are audit routines that flag suspicious transactions.
- ❖ Example: State Farm Life Insurance looking for policyholders who change their name or address and then subsequently withdraw funds.
- ❖ When audit hooks are used, auditors can be informed of questionable transactions as they occur via ***real-time notification***, which displays a message on the auditor's terminal.

Audit Hooks



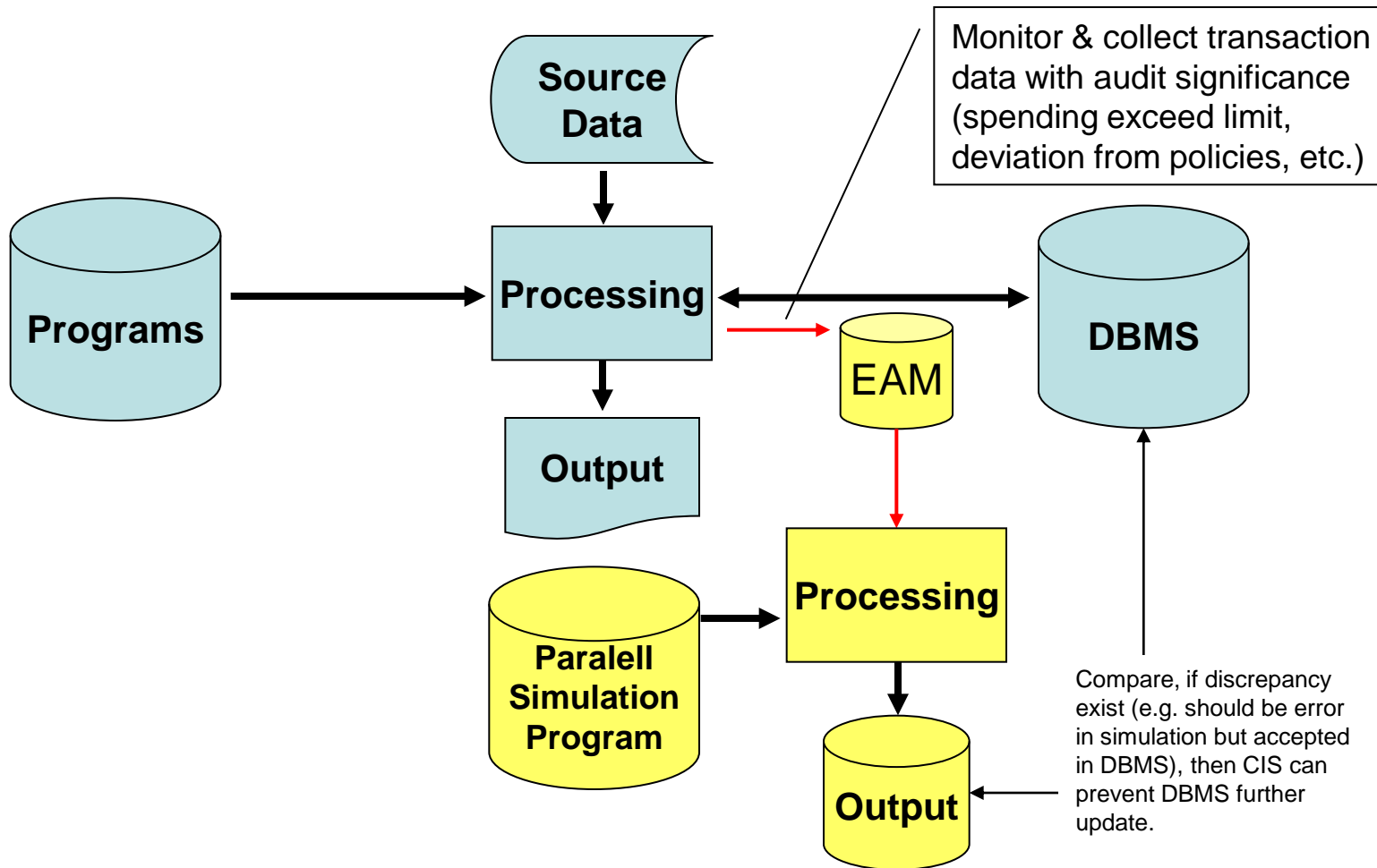
❖ Auditors commonly use five concurrent audit techniques:

- An integrated test facility (ITF) technique
- A snapshot technique
- A system control audit review file (SCARF)
- **Audit hooks**
- **Continuous and intermittent simulation (CIS)**

OBJECTIVE 4: COMPUTER PROCESSING

- ❖ ***Continuous and intermittent simulation (CIS)*** embeds an audit module in a database management system.
- ❖ The module examines all transactions that update the DBMS using criteria similar to those of SCARF.
- ❖ When a transaction has audit significance, the module:
 - Processes the data independently (similar to parallel simulation);
 - Records the results;
 - Compares results with those obtained by the DBMS.
- ❖ If there are discrepancies, details are written to an audit log for subsequent investigation.
- ❖ Serious discrepancies may prevent the DBMS from executing the update.

Continuous and Intermittent Simulation (CIS)



OBJECTIVE 4: COMPUTER PROCESSING

❖ Analysis of Program Logic


- If an auditor suspects that a particular program contains unauthorized code or serious errors, a detailed analysis of the program logic may be necessary.
- Done only as a last resort because:
 - It's time-consuming
 - Requires programming language proficiency
- To perform the analysis, auditors reference:
 - Program flowcharts
 - Program documentation
 - Program source code.

OBJECTIVE 4: COMPUTER PROCESSING

❖ **The following software packages can help:**

- **Automated flowcharting programs**

- Interpret program source code and generate a corresponding flowchart.



OBJECTIVE 4: COMPUTER PROCESSING

❖ The following software packages can help:

- Automated flowcharting programs
- **Automated decision table programs**
 - Generates a decision table that represents the program logic.

OBJECTIVE 4: COMPUTER PROCESSING

❖ The following software packages can help:

- Automated flowcharting programs
- Automated decision table programs
- **Scanning routines**

- Search programs for specified variable names or character combinations.

❖ The following software packages can help:

- Automated flowcharting programs
- Automated decision table programs
- Scanning routines
- **Mapping programs**

- Identify unexecuted program code.

OBJECTIVE 4: COMPUTER PROCESSING

❖ The following help:

- Automation
- Automation
- Scanning
- Mapping

- **Program tracing**

- ❖ Sequentially prints all program steps executed during a program run.
- ❖ This list is intermingled with regular output so auditors can observe the precise sequence of events that unfold during program execution.
- ❖ Helps auditors detect:
 - Unauthorized program instructions
 - Incorrect logic paths
 - Unexecuted program code

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

Files

Objective 3:
Program Modification

Objective 4: Computer Processing

Objective 6:
Data Files

Objective 5: Source Data



IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source
Data

Data
Entry

Objective 2:
Program Development
And Acquisition

Source
Data

Programs

Processing

Files

Output

Objective 3:
Program Modification

Objective 4: Computer Processing

Objective 6:
Data Files



OBJECTIVE 5: SOURCE DATA

❖ Types of Errors and Fraud

- Inaccurate source data
- Unauthorized source data

OBJECTIVE 5: SOURCE DATA

❖ Control 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 for user department review
- Effective procedures for correcting and resubmitting erroneous data

OBJECTIVE 5: SOURCE DATA

❖ Audit 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 an input control matrix
- Discuss source data control procedures with data control personnel as well as the users and managers of the system

OBJECTIVE 5: SOURCE DATA

❖ Audit 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 handled
- 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

OBJECTIVE 5: SOURCE DATA

❖ **Compensating Controls**

- Strong user controls
- Strong processing controls



OBJECTIVE 5: SOURCE DATA

- Auditors use an ***input controls matrix*** (as shown on the next slide) to document the review of source data controls.
- The matrix shows the control procedures applied to each field of an input record.

Record Name	Field Names							Comments	
	Employee Weekly Time Report	Employee Number	Last Name	Department Number	Transaction Number	Week Ending Code	Week Ending (Date)		Regular Hours
Input Controls									
Financial totals						✓	✓		
Hash totals	✓								
Record counts									Yes
Cross-footing balance									No
Key verification	✓					✓	✓		
Visual inspection									All fields
Check digit verification	✓								
Pre-numbered forms									No
Turnaround document									No
Edit program									Yes
Sequence check	✓								
Field check	✓		✓			✓	✓		
Sign check									
Validity check	✓		✓	✓	✓				
Limit check						✓	✓		
Reasonableness test						✓	✓		
Redundant data check	✓	✓	✓						
Completeness test				✓	✓	✓	✓		
Overflow procedure									
Other									

OBJECTIVE 5: SOURCE DATA

- ❖ **Auditors should ensure the data control function:**
 - Is independent of other functions
 - Maintains a data control log
 - Handles errors
 - Ensures overall efficiency of operations
- ❖ Usually not feasible for small businesses and PC installations to have an independent data control function.

OBJECTIVE 5: SOURCE DATA

- ❖ **To compensate, user department controls must be stronger over:**
 - Data preparation
 - Batch control totals
 - Edit programs
 - Physical and logical access restrictions
 - Error handling procedures
- ❖ These procedures should be the focus of the auditor's systems review and tests of controls when there is no independent data control function.



OBJECTIVE 5: SOURCE DATA

- ❖ Auditors should test source data controls on a regular basis, because the strictness with which they are applied may vacillate.
 - Samples should be evaluated for proper authorization.
 - A sample of batch control totals should also be reconciled.
 - A sample of data edit errors should be evaluated to ensure they were resolved and resubmitted.

OBJECTIVE 5: SOURCE DATA

- ❖ Auditors should test source data controls on a regular basis, because the strictness with which they are applied may vacillate.
- ❖ Samples should be evaluated for proper authorization.
- ❖ A sample of batch controls should also be reconciled.
- ❖ A sample of data edit errors should be evaluated to ensure they were resolved and resubmitted.
- ❖ If source data controls are inadequate, user department and computer processing controls may compensate.
- ❖ Otherwise, the auditor should strongly recommend steps to correct the deficiencies.

IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source
Data

Data
Entry

Objective 2:
Program Development
And Acquisition

Source
Data

Programs

Processing

Files

Output

Objective 3:
Program Modification

Objective 4: Computer Processing

Objective 6:
Data Files

Objective 6: Data Files



IS COMPONENTS AND AUDIT OBJECTIVES

Objective 1: Overall Security

Objective 5: Source Data

Source Data

Data Entry

Source Data

Processing

Output

Objective 2:
Program Development
And Acquisition

Programs

Objective 3:
Program Modification

Objective 4: Computer Processing

Files

Objective 6:
Data Files

OBJECTIVE 6: DATA FILES

- ❖ The sixth objective concerns the accuracy, integrity, and security of data stored in machine-readable files.
- ❖ Data storage risks include:
 - Unauthorized modification of data
 - Destruction of data
 - Disclosure of data
- ❖ Many of the controls discussed in session 8 protect against the preceding risks.
- ❖ If file controls are seriously deficient, especially with respect to access or backup and recovery, the auditor should strongly recommend they be rectified.

OBJECTIVE 6: DATA FILES

- ❖ ***Auditing-by-objectives*** is a comprehensive, systematic, and effective means of evaluating internal controls in an application.
 - Can be implemented using an audit procedures checklist for each objective.
 - Should help the auditor reach a separate conclusion for each objective and suggest compensating controls.
- ❖ A separate version of the checklist should be completed for each significant application.

OBJECTIVE 6: DATA FILES

- ❖ Auditors should review system designs while their suggestions can be incorporated.
- ❖ Techniques such as ITF, snapshot, SCARF, audit hooks, and real-time notification should be incorporated during design.
- ❖ It is much more difficult and costly to add them later.

❖ Types of Errors and Fraud

- Destruction of stored data due to:
 - Inadvertent errors
 - Hardware or software malfunctions
 - Intentional acts of sabotage or vandalism
- Unauthorized modification or disclosure of stored data

OBJECTIVE 6: DATA FILES

❖ 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
- Encryption of highly confidential data
- Use of virus protection software
- Maintenance of backup copies of all data files in an off-site location

OBJECTIVE 6: DATA FILES

❖ 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 storage
 - System recovery, including checkpoint and rollback procedures

OBJECTIVE 6: DATA FILES

- 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 systems managers and operators

OBJECTIVE 6: DATA FILES

❖ 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

OBJECTIVE 6: DATA FILES

❖ **Compensating Controls**

- Strong user controls
- Effective computer security controls
- Strong processing controls

Computer Audit Software



- ❖ Questions to be addressed in this session include:
 - What are the scope and objectives of audit work, and what major steps take place in the audit process?
 - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
 - How can a plan be designed to study and evaluate internal controls in an application?
 - **How can computer audit software be useful in the audit of an application?**
 - What is the nature and scope of an operational audit?

- ❖ **Computer audit software (CAS)** or **generalized audit software (GAS)** are computer programs that have been written especially for auditors.
- ❖ Two of the most popular:
 - Audit Control Language (ACL)
 - IDEA
- ❖ Based on auditor's specifications, CAS generates programs that perform the audit function.
- ❖ CAS is ideally suited for examination of large data files to identify records needing further audit scrutiny.

❖ CAS functions include:

- **Reformatting**

- **Converting data into a different format or structure to facilitate testing.**

❖ CAS functions include:

- Reformatting
- **File manipulation**

- **Sorting records or merging records from different files.**

❖ CAS functions include:

- Reformatting
- File manipulation
- **Calculation**

- Performing arithmetic operations on the data.

❖ CAS functions include:

- Reformatting
- File manipulation
- Calculation
- **Data selection**

- Retrieving records that meet specific criteria.

❖ CAS functions include:

- Reformatting
- File manipulation
- Calculation
- Data selection
- **Data analysis**

- ❖ Examining data for errors or missing values.
- ❖ Comparing fields in related records for inconsistencies.

❖ CAS functions include:

- Reformatting
- File manipulation
- Calculation
- Data selection
- Data analysis
- **File processing**

- Programming to create, update, and download files to a personal computer.

❖ CAS functions include:

- Reformatting
- File manipulation
- Calculation
- Data selection
- Data analysis
- File processing
 - Stratifying file records on various criteria, selecting statistical samples, and analyzing statistical results.
- **Statistics**

❖ CAS functions include:

- Reformatting
 - File manipulation
 - Calculation
 - Data selection
 - Data analysis
 - File processing
 - Statistics
 - **Report generation**
- **Formatting and printing reports and documents.**

❖ How CAS is used:

- The auditor:
 - Decides on audit objectives;
 - Learns about the files and databases to be audited;
 - Designs the audit reports; and
 - Determines how to produce them.
- This information is recorded on specification sheets and entered into the system.
- The program creates specification records used to produce auditing programs.
- The auditing programs process the source files and produce specified audit reports.

COMPUTER SOFTWARE

- ❖ The primary purpose of CAS is to assist the auditor in reviewing and retrieving information.
- ❖ When the auditor receives the CAS reports, most of the audit work still needs to be done.
 - Items on exception reports must be investigated.
 - File totals must be verified against other sources.
 - Audit samples must be examined and evaluated.
- ❖ Advantages of CAS are numerous, but it does not replace the auditor's judgment or free the auditor from other phases of the audit.

Operational Audit of An Application




- ❖ Questions to be addressed in this session include:
 - What are the scope and objectives of audit work, and what major steps take place in the audit process?
 - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
 - How can a plan be designed to study and evaluate internal controls in an application?
 - How can computer audit software be useful in the audit of an application?
 - **What is the nature and scope of an operational audit?**

OPERATIONAL AUDITS OF AN APPLICATION

- ❖ Techniques and procedures in operational audits are similar to audits of information systems and financial statement audits.
- ❖ The scope is different.
 - IS audit scope is confined to internal controls
 - Financial audit scope is limited to system output.
 - Operational audit scope is much broader and encompasses all aspects of information systems management.
- ❖ Objectives are also different in that operational audit objectives include evaluating factors such as:
 - Effectiveness
 - Efficiency
 - Goal achievement

OPERATIONAL AUDITS OF AN APPLICATION

- ❖ First step in an operational audit is audit planning, which includes:
 - Setting scope and objective of audit
 - Performing preliminary review of system
 - Preparing tentative audit program.




OPERATIONAL AUDITS OF AN APPLICATION

- ❖ Next step is evidence collection, which includes:
 - Reviewing operating policies and documentation
 - Confirming procedures with management and operating personnel
 - Observing operating functions and activities
 - Examining financial and operating plans and reports
 - Testing accuracy of operating information
 - Testing controls

OPERATIONAL AUDITS OF AN APPLICATION

- ❖ In the evidence evaluation stage, the auditor measures the actual system against an ideal one (best practices).
 - An important consideration is that results are more significant than the policies and practices themselves.
 - If good results are achieved through deficient policies and practices, the auditor must carefully consider whether recommended improvements would substantially improve results.
- Finally, the auditor should thoroughly document findings and conclusions and communicate audit results to management.



OPERATIONAL AUDITS OF AN APPLICATION

- ❖ The ideal operational auditor is a person with audit training and some managerial experience.
- ❖ Those with strong auditing backgrounds but weak or no management experience often lack necessary perspective.

- ❖ In this session, you've learned about the scope and objectives of audit work and the major steps that take place in the audit process.
- ❖ You've also learned about the objectives of an information systems audit and the four-step approach for meeting those objectives.
- ❖ You've learned how a plan can be designed to study and evaluate internal controls in an application and how computer audit software can be useful in the audit of an application.
- ❖ Finally, you've learned about the nature and scope of an operational audit.