



# **Accounting Information Systems**

PRESENTED BY: EDGAR OTIENO

## **Lecture 6 SECURITY**

**Computer Controls and Auditing:  
IT Controls Parts I and II**

# background

- Local news: <https://kenyandigest.com/cma-how-chase-bank-chiefs-siphoned-billions/>

# Objectives for Lecture 6

- **IT Controls Part I: Security and Access**
  - Threats to the operating system and internal controls (IC) to minimize them
  - Threats to database integrity and IC to minimize them
  - Risks associated with electronic commerce and IC to reduce them
- **IT Controls Part II: Systems Development, Program Changes, and Application Controls**
  - Controls and audit tests relevant to systems development
  - Risks and controls for program changes and the source program library
  - Auditing techniques (CAATTs) used to verify application controls
  - Auditing techniques used to perform substantive tests in an IT environment



# Goals of Security

- Authorization
- Authentication
- Non repudiation
- Integrity
- Availability
- Confidentiality



## **(1) IT Controls Part I: Security and Access**

# Operating Systems

- Perform three main tasks:
  - translates high-level languages into the machine-level language
  - allocates computer resources to user applications
  - manages the tasks of job scheduling and multiprogramming



# Requirements for Effective Operating Systems Performance

- Protect itself from tampering from users
- Prevent users from tampering with the programs of other users
- Safeguard users' applications from accidental corruption
- Safeguard its own programs from accidental corruption
- Protect itself from power failures and other disasters

# Operating Systems Security

- **Log-On Procedure**
  - first line of defence – user IDs and passwords
- **Access Token**
  - contains key information about the user
- **Access Control List**
  - defines access privileges of users
- **Discretionary Access Control**
  - allows user to grant access to another user



# Operating Systems Controls

## Access Privileges

- *Audit objectives:* verify that access privileges are consistent with separation of incompatible functions and organization policies
- *Audit procedures:* review or verify...
  - policies for separating incompatible functions
  - a sample of user privileges, especially access to data and programs
  - security clearance checks of privileged employees
  - formally acknowledgements to maintain confidentiality of data
  - users' log-on times

# Operating Systems S Controls

## Password Control

- *Audit objectives*: ensure adequacy and effectiveness password policies for controlling access to the operating system
- *Audit procedures*: review or verify...
  - passwords required for all users
  - password instructions for new users
  - passwords changed regularly
  - password file for weak passwords
  - encryption of password file
  - password standards
  - account lockout policies

# Operating Systems Controls

## Malicious & Destructive Programs

- *Audit objectives:* verify effectiveness of procedures to protect against programs such as viruses, worms, back doors, logic bombs, and Trojan horses
- *Audit procedures:* review or verify...
  - training of operations personnel concerning destructive programs
  - testing of new software prior to being implemented
  - currency of antiviral software and frequency of upgrades



# Operating System Controls

## Audit Trail Controls

- *Audit objectives*: whether used to (1) detect unauthorized access, (2) facilitate event reconstruction, and (3) promote accountability
- *Audit procedures*: review or verify...
  - how long audit trails have been in place
  - archived log files for key indicators
  - monitoring and reporting of security violations

# Database Management Controls

**Two crucial database control issues:**

## **Access controls**

- *Audit objectives:* (1) those authorized to use databases are limited to data needed to perform their duties and (2) unauthorized individuals are denied access to data

## **Backup controls**

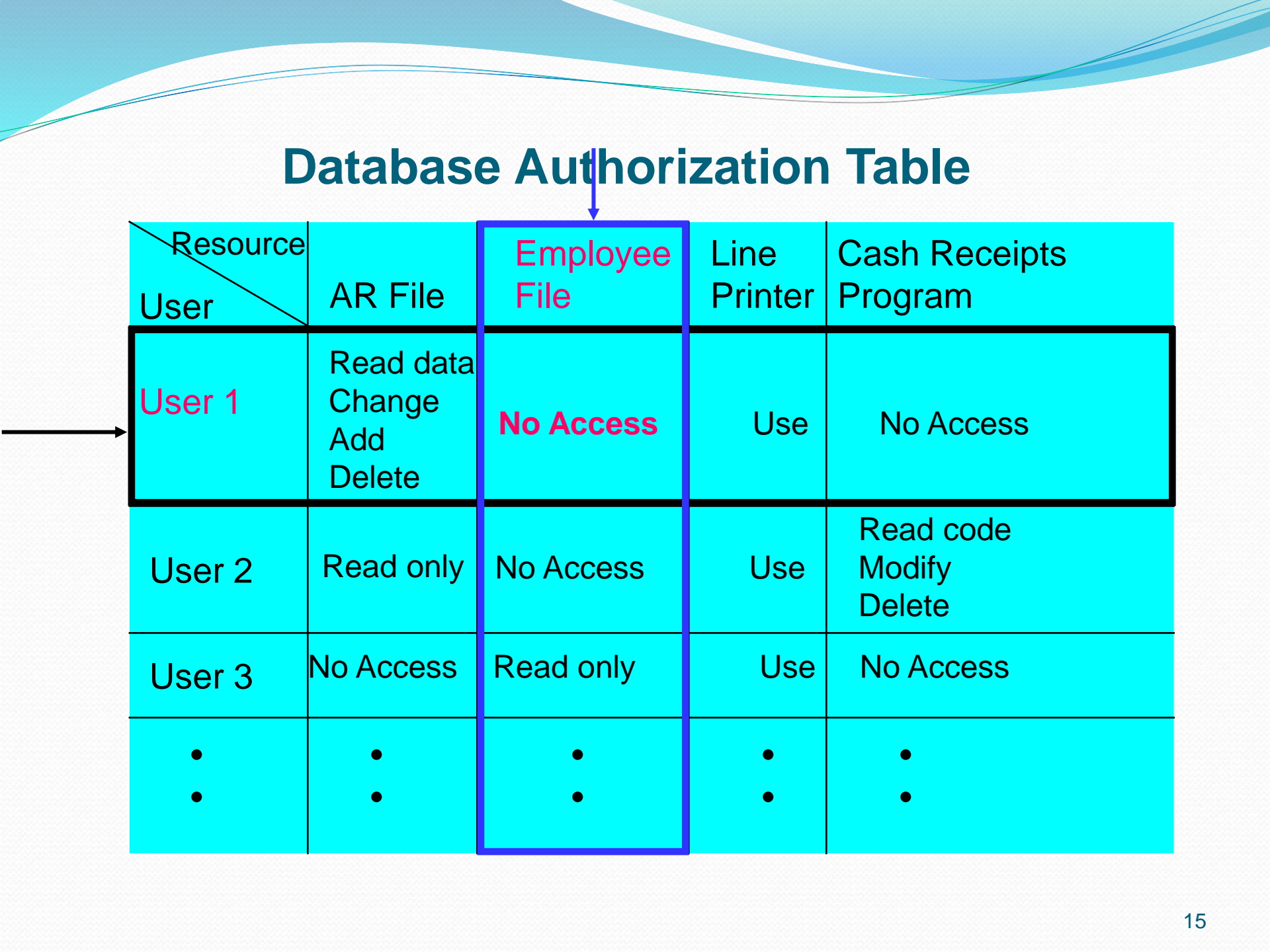
- *Audit objectives:* backup controls can adequately recovery lost, destroyed, or corrupted data

# Access Controls

- **User views** - based on sub-schemas
- **Database authorization table** - allows greater authority to be specified
- **User-defined procedures** - user to create a personal security program or routine
- **Data encryption** - encoding algorithms
- **Biometric devices** - fingerprints, retina prints, or signature characteristics



# Database Authorization Table



Resource User	AR File	Employee File	Line Printer	Cash Receipts Program
User 1	Read data Change Add Delete	No Access	Use	No Access
User 2	Read only	No Access	Use	Read code Modify Delete
User 3	No Access	Read only	Use	No Access
• •	• •	• •	• •	• •

# Access Controls

*Audit procedures: verify...*

- responsibility for authority tables & subschemas
- granting appropriate access authority
- use or feasibility of biometric controls
- use of encryption

# Backup Controls

- **Database backup** – automatic periodic copy of data
- **Transaction log** – list of transactions which provides an audit trail
- **Checkpoint features** – suspends data during system reconciliation
- **Recovery module** – restarts the system after a failure



# Backup Controls

*Audit procedures: verify...*

- that production databases are copied at regular intervals
- backup copies of the database are stored off site to support disaster recovery

# Internet and Intranet Risks

- Communications is a unique aspect of the computer networks:
  - different than processing (applications) or data storage (databases)
- Network topologies – configurations of:
  - communications lines (twisted-pair wires, coaxial cable, microwaves, fiber optics)
  - hardware components (modems, multiplexers, servers, front-end processors)
  - software (protocols, network control systems)

# Sources of Internet & Intranet Risks

## Internal and external subversive activities

*Audit objectives:*

1. prevent and detect illegal internal and external network access
2. render useless any data captured by a perpetrator
3. preserve the integrity and physical security of data connected to the network

## Equipment failure

*Audit objective:*

the integrity of the electronic commerce transactions by determining that controls are in place to detect and correct message loss due to equipment failure



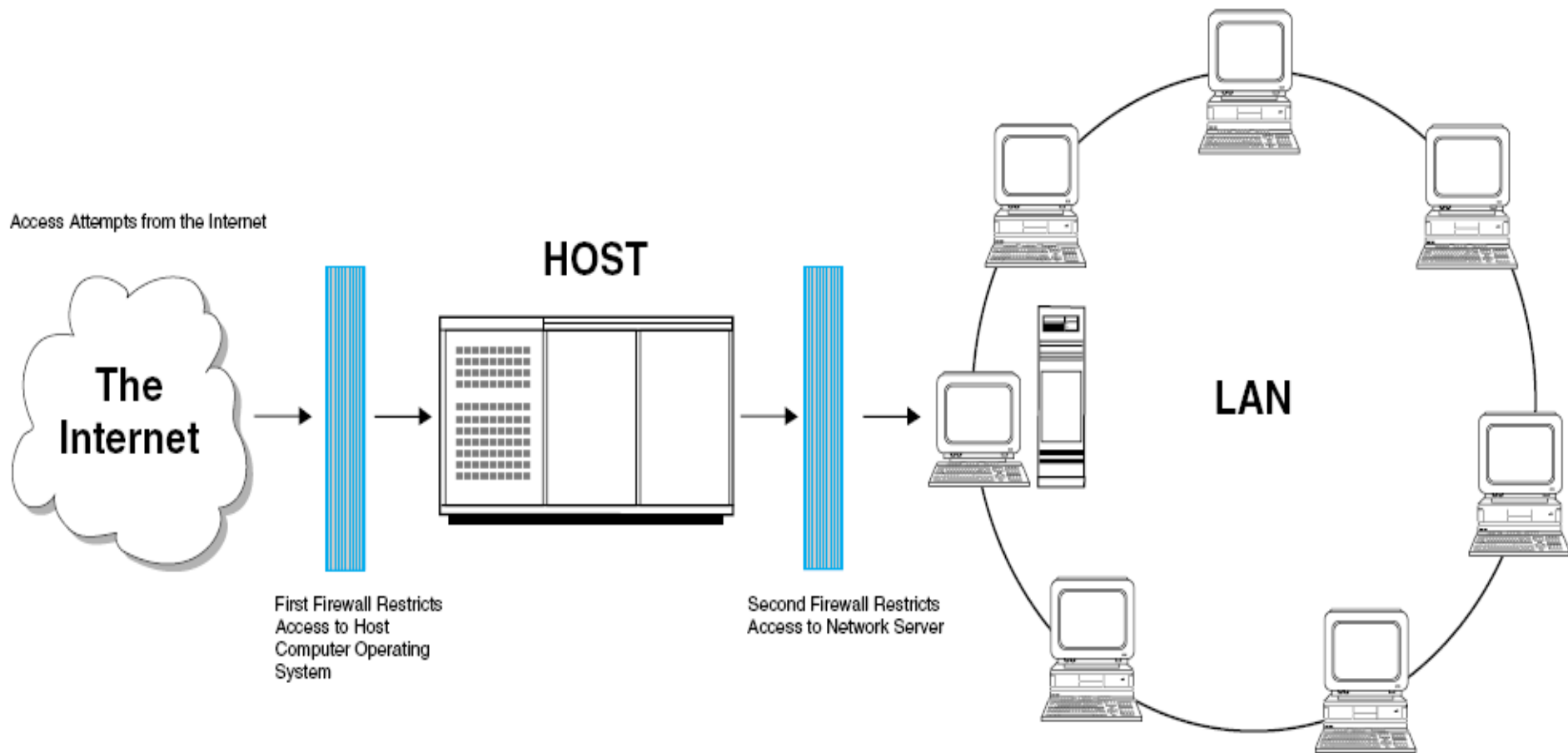
# Risks from Subversive Threats

- Include:
  - unauthorized interception of a message
  - gaining unauthorized access to an organization's network
  - a denial-of-service attack from a remote location

# Internal Controls for Subversive Threats

- Firewalls provide security by channeling all network connections through a control gateway.
  - Network level firewalls
    - Low cost and low security access control
    - Do not explicitly authenticate outside users
    - Filter junk or improperly routed messages
    - Experienced hackers can easily penetrate the system
  - Application level firewalls
    - Customizable network security, but expensive
    - Sophisticated functions such as logging or user authentication

# Dual-Homed Firewall





# Internal Controls for Subversive Threats

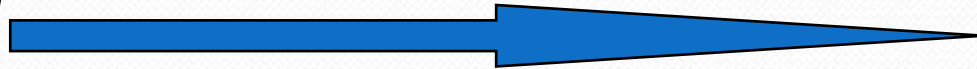
- **Denial-of-service (DOS) attacks**
  - Security software searches for connections which have been half-open for a period of time.
- **Encryption**
  - Computer program transforms a clear message into a coded (cipher) text form using an algorithm.

# DOS Attack

**Sender**



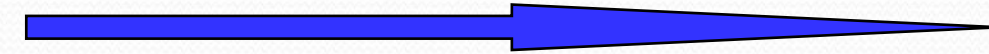
**Step 1: SYN messages**



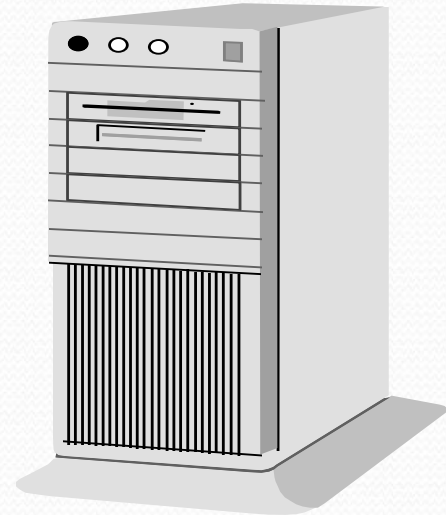
**Step 2: SYN/ACK**



**Step 3: ACK packet code**

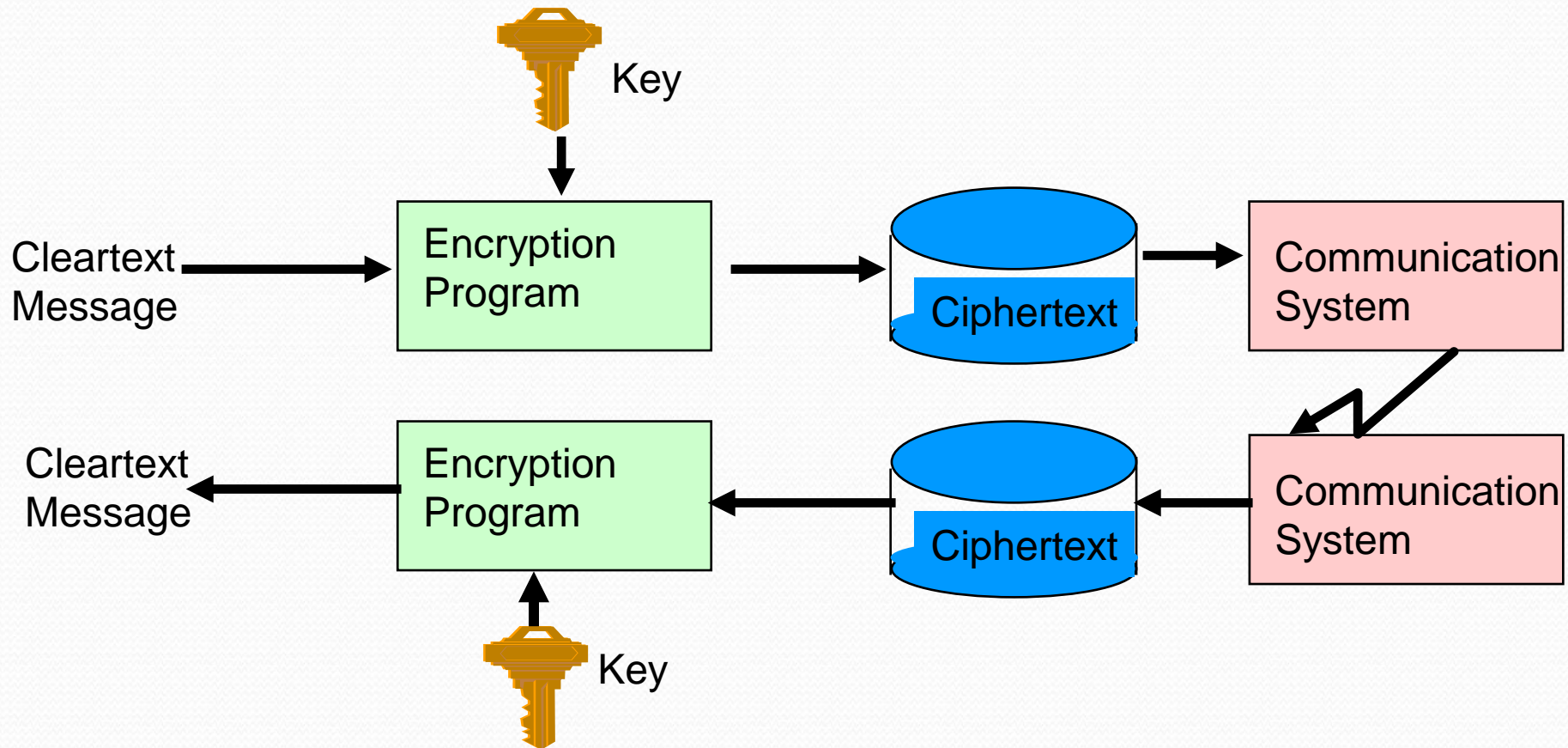


**Receiver**



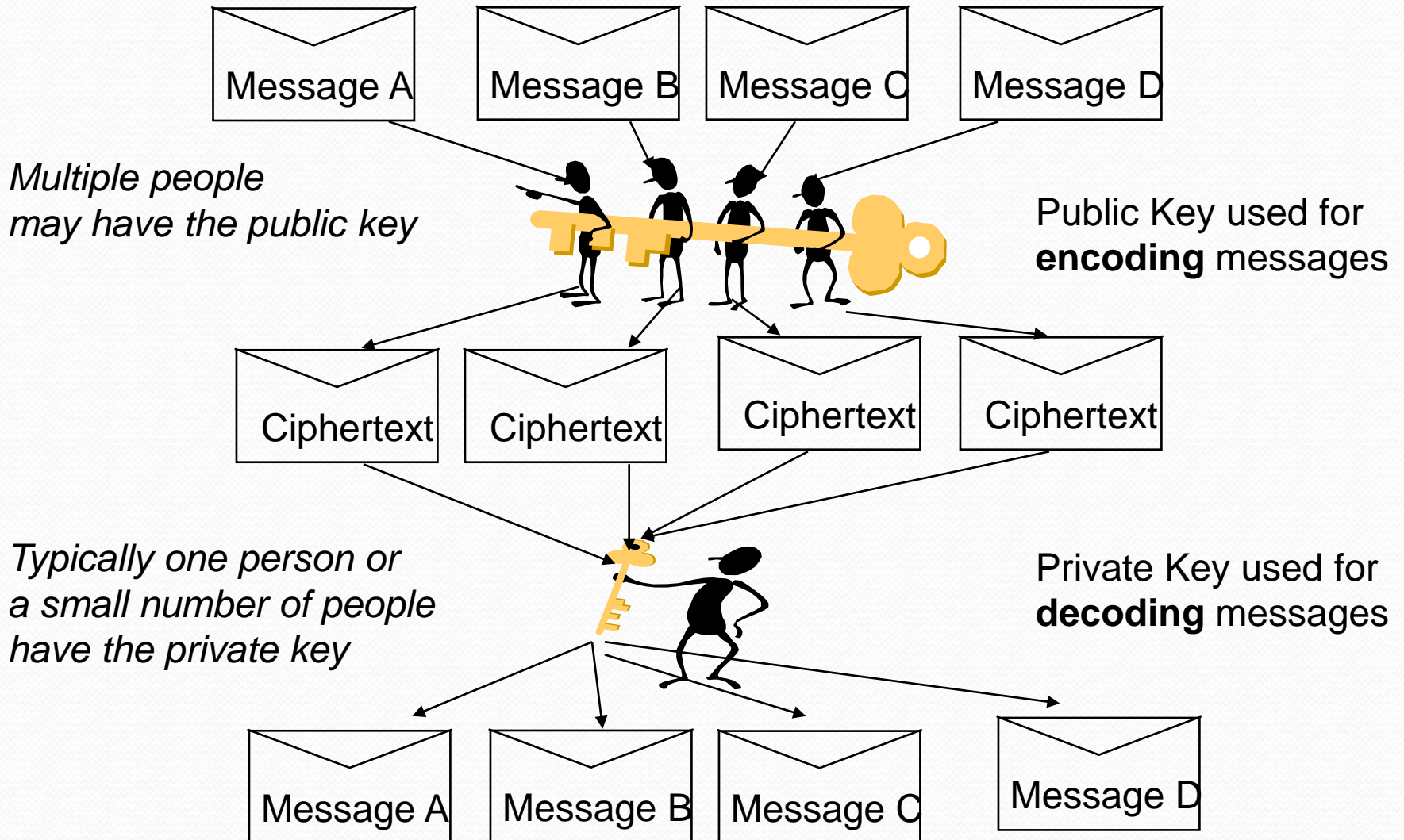
In a DOS Attack, the sender sends hundreds of messages, receives the SYN/ACK packet, but does not response with an ACK packet. This leaves the receiver with clogged transmission ports, and legitimate messages cannot be received.

# Standard Data Encryption Technique



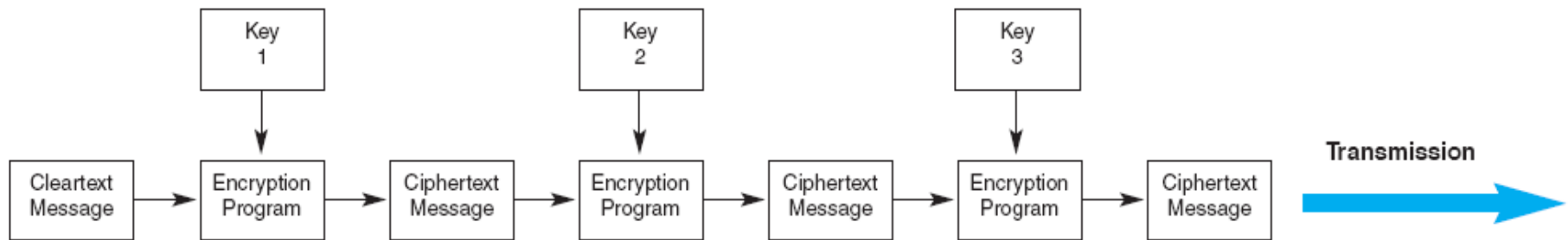


# Public – Private Key Encryption

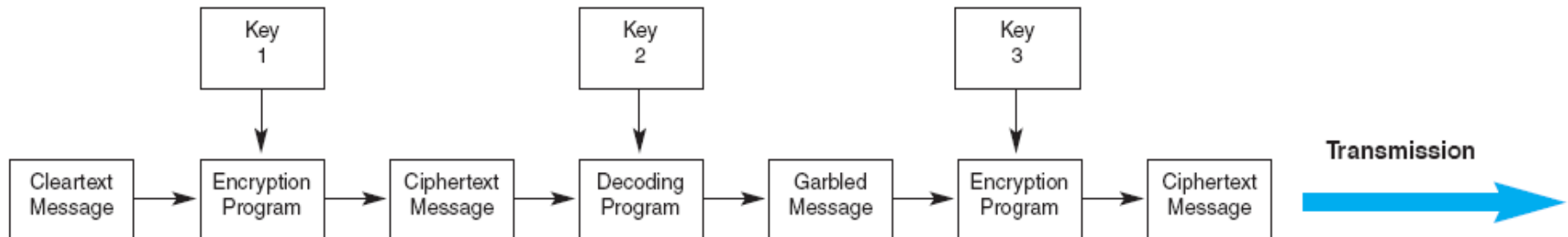


# Advanced Data Encryption Technique

EEE3 Technique



EDE3 Technique

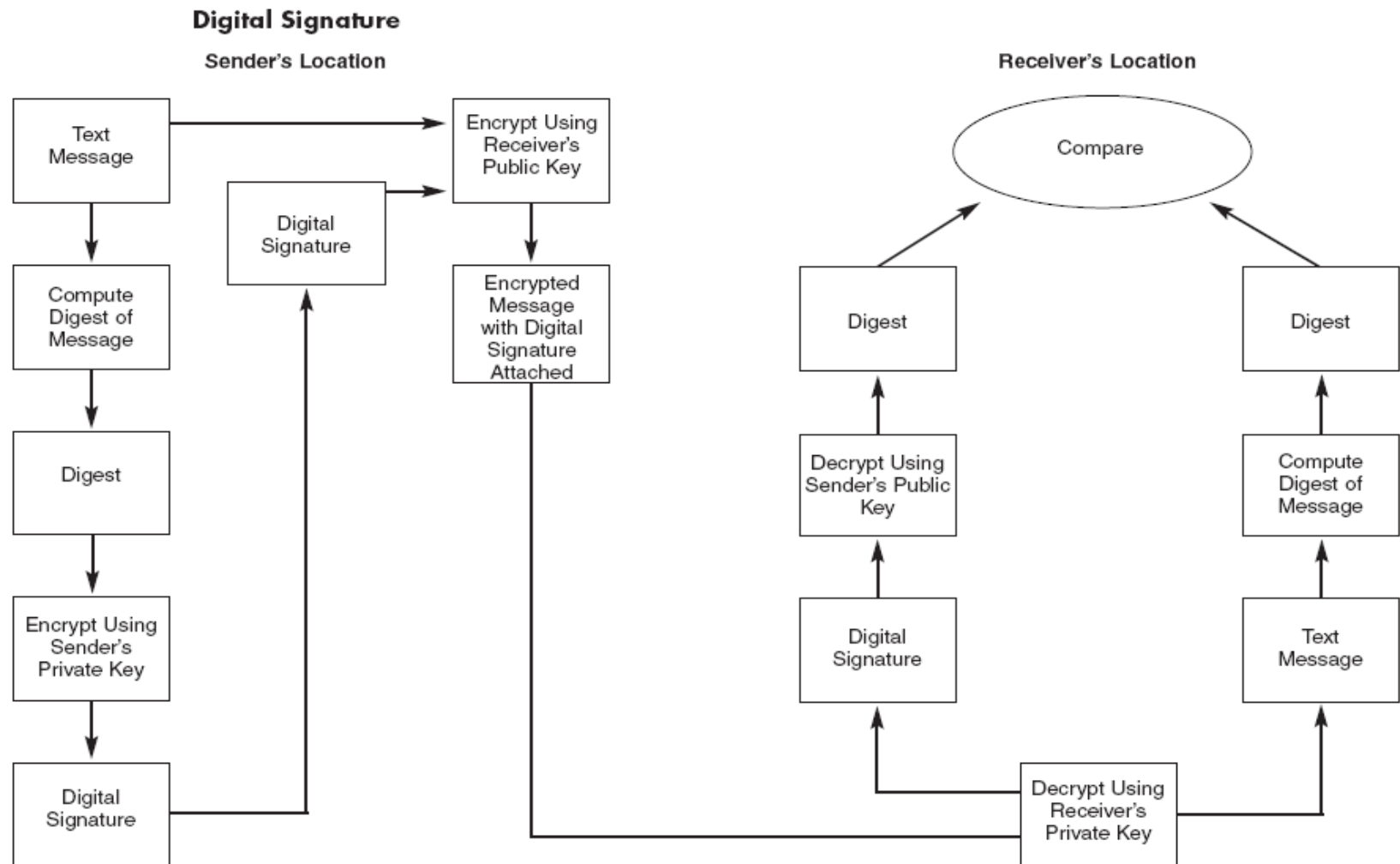


# Internal Controls for Subversive Threats

- **Digital signature** – electronic authentication technique to ensure that...
  - transmitted message originated with the authorized sender
  - message was not tampered with after the signature was applied
- **Digital certificate** – like an electronic identification card used with a public key encryption system
  - Verifies the authenticity of the message sender



# Digital Signature



# Auditing Procedures for Subversive Threats

- Review firewall effectiveness in terms of flexibility, proxy services, filtering, segregation of systems, audit tools, and probing for weaknesses.
- Review data encryption security procedures
- Verify encryption by testing
- Review message transaction logs
- Test procedures for preventing unauthorized calls

# IC for Equipment Failure

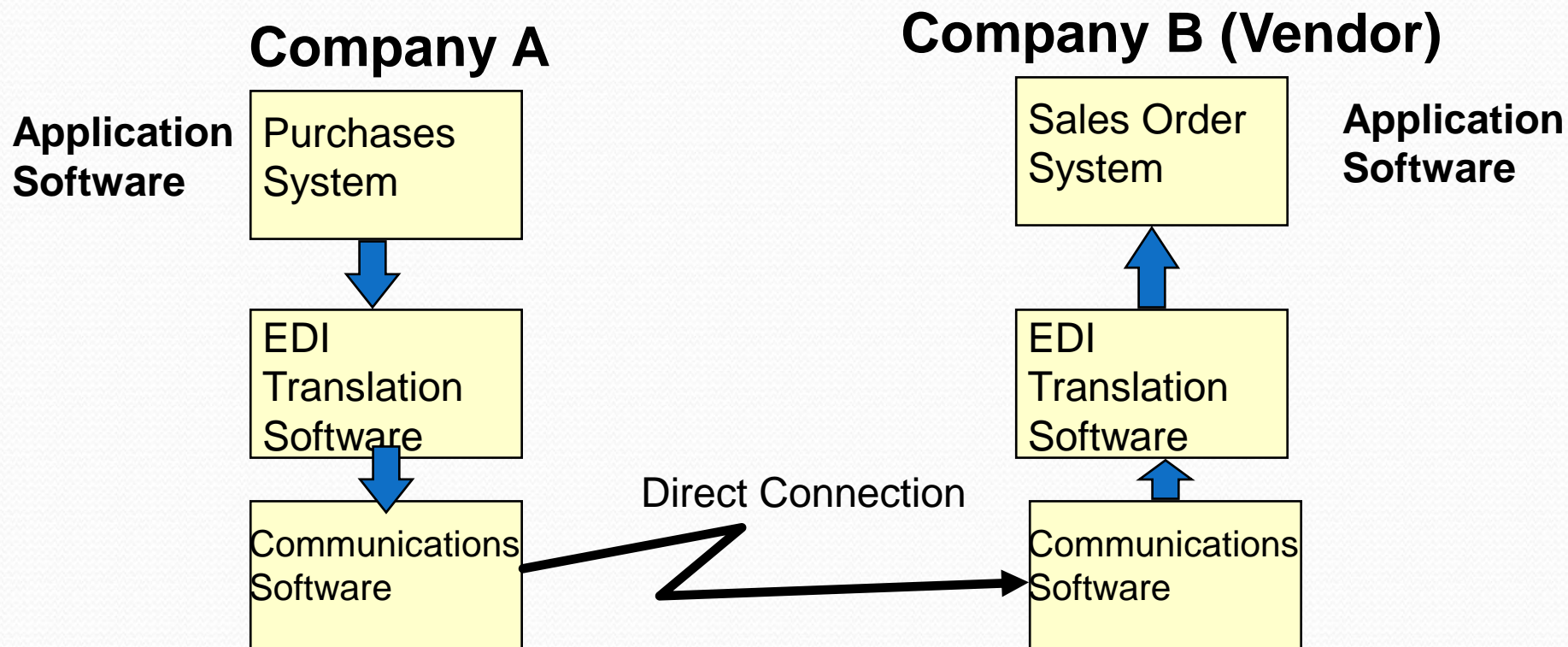
- Line errors are data errors from communications noise.
- Two techniques to detect and correct such data errors are:
  - echo check - the receiver returns the message to the sender
  - parity checks - an extra bit is added onto each byte of data similar to check digits



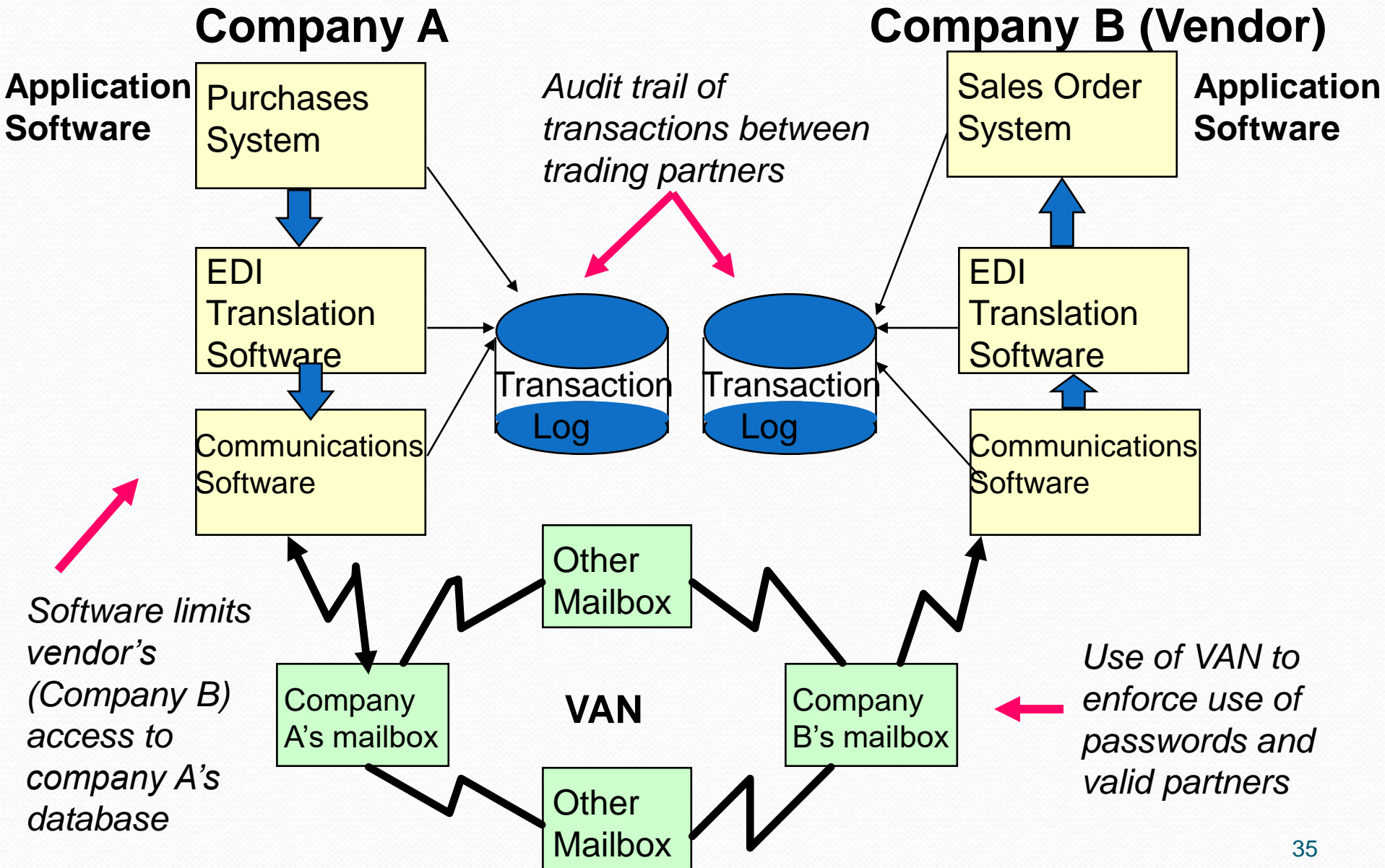
# Electronic Data Interchange

- Electronic data interchange (EDI) uses computer-to-computer communications technologies to automate B2B purchases.
- Audit objectives:
  1. Transactions are authorized, validated, and in compliance with the trading partner agreement.
  2. No unauthorized organizations can gain access to database
  3. Authorized trading partners have access only to approved data.
  4. Adequate controls are in place to ensure a complete audit trail.

# EDI System without Controls



# EDI System with Controls





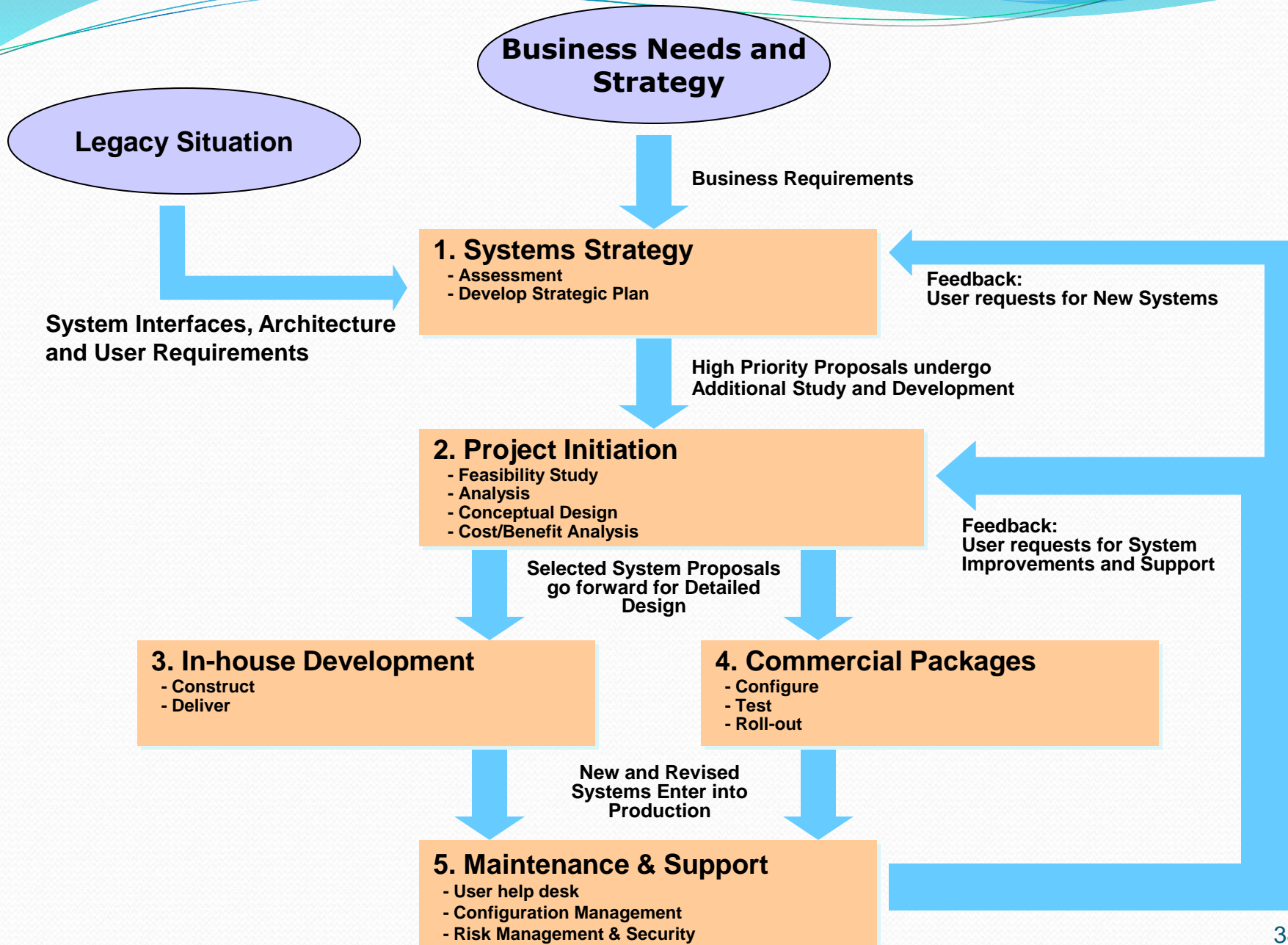


## **(2) IT Controls Part II: Systems Development, Program Changes, and Application Controls**

# Systems Development Activities

- Authorizing development of new systems
- Addressing and documenting user needs
- Technical design phases
- Participation of internal auditors
- Testing program modules before implementing
  - Testing individual modules by a team of users, internal audit staff, and systems professionals

# Systems Development Life Cycle





# Systems Development

## **Auditing objectives:** ensure that...

- SDLC activities are applied consistently and in accordance with management's policies
- the system as originally implemented was free from material errors and fraud
- the system was judged to be necessary and justified at various checkpoints throughout the SDLC
- system documentation is sufficiently accurate and complete to facilitate audit and maintenance activities

# Systems Development IC

- New systems must be authorized.
- Feasibility studies were conducted.
- User needs were analyzed and addressed.
- Cost-benefit analysis was done.
- Proper documentation was completed.
- All program modules must be thoroughly tested before they are implemented.
- Checklist of problems was kept.

# System Maintenance IC

- Last, longest and most costly phase of SDLC
  - Up to 80-90% of entire cost of a system
- All maintenance actions should require
  - Technical specifications
  - Testing
  - Documentation updates
  - Formal authorizations for any changes



# Program Change

**Auditing objectives:** detect unauthorized program maintenance and determine that...

- maintenance procedures protect applications from unauthorized changes
- applications are free from material errors
- program libraries are protected from unauthorized access

# Program Change

- **Auditing procedures:** verify that programs were properly maintained, including changes
- Specifically, verify...
  - identification and correction of unauthorized program changes
  - identification and correction of application errors
  - control of access to systems libraries

# Application Controls

- **Narrowly focused exposures within a specific system, for example:**
  - accounts payable
  - cash disbursements
  - fixed asset accounting
  - payroll
  - sales order processing
  - cash receipts
  - general ledger



# Application Controls

- Risks within specific applications
- Can affect manual procedures (e.g., entering data) or embedded (automated) procedures
- Convenient to look at in terms of:
  - input stage
  - processing stage
  - output stage



# Application Input Controls

- Goal of input controls - valid, accurate, and complete input data
- Two common causes of input errors:
  - transcription errors – wrong character or value
  - transposition errors – ‘right’ character or value, but in wrong place

# Application Input Controls

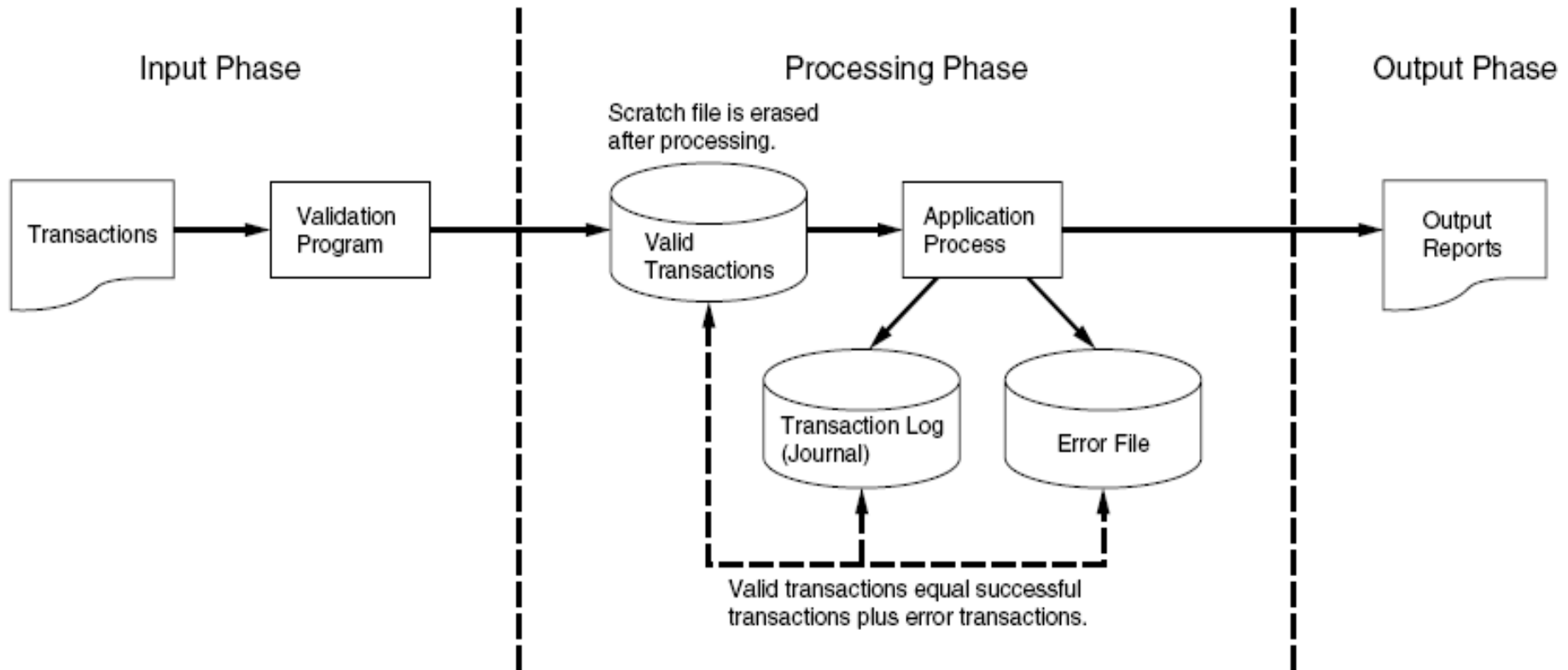
- Check digits – data code is added to produce a control digit
  - especially useful for transcription and transposition errors
- Missing data checks – control for blanks or incorrect justifications
- Numeric-alphabetic checks – verify that characters are in correct form



# Application Input Controls

- Limit checks – identify values beyond pre-set limits
- Range checks – identify values outside upper and lower bounds
- Reasonableness checks – compare one field to another to see if relationship is appropriate
- Validity checks – compares values to known or standard values

# Transaction Log to Preserve the Audit Trail



# Application Output Controls

- Goal of output controls is to ensure that system output is not lost, misdirected, or corrupted, and that privacy is not violated.
- In the following flowchart, there are exposures at every stage.



# Application Controls Output

- **Waste** – can be stolen if not properly disposed of, e.g., shredding
- **Report distribution** – for sensitive reports, the following are available:
  - use of secure mailboxes
  - require the user to sign for reports in person
  - deliver the reports to the user

# Application Controls Output

- **End user controls** – end users need to inspect sensitive reports for accuracy
  - shred after used
- **Controlling digital output** – digital output message can be intercepted, disrupted, destroyed, or corrupted as it passes along communications links

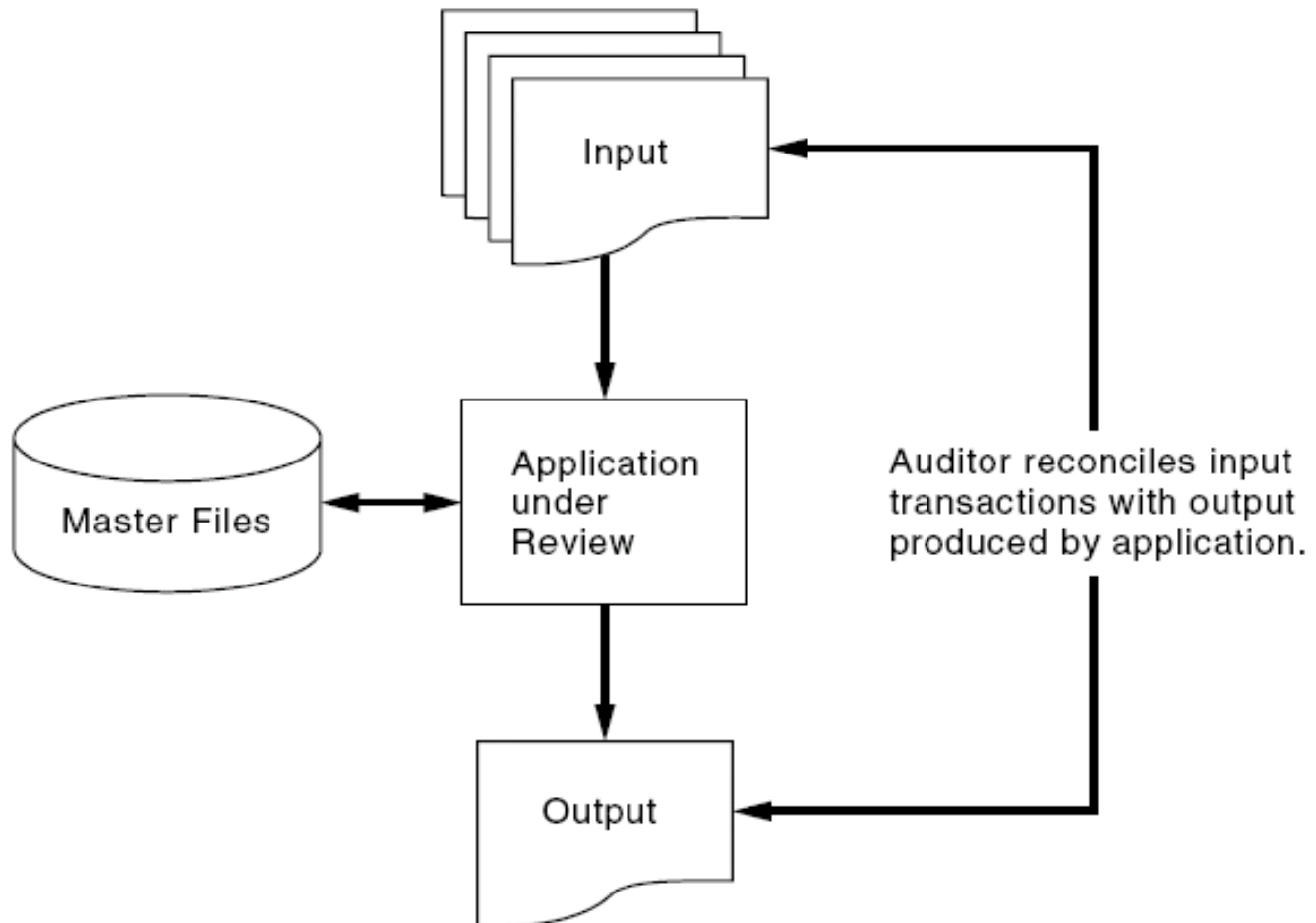
# Testing Application Controls

Techniques for auditing applications fall into two classes:

- 1) testing application controls – two general approaches:
  - black box – around the computer
  - white box – through the computer
- 2) examining transaction details and account balances –  
*substantive testing*



# Auditing Around the Computer - The Black Box Approach



# Testing Application Controls

- **Black Box Approach** – focuses on input procedures and output results
- To Gain need understanding...
  - analyze flowcharts
  - review documentation
  - conduct interviews

# Testing Application Controls

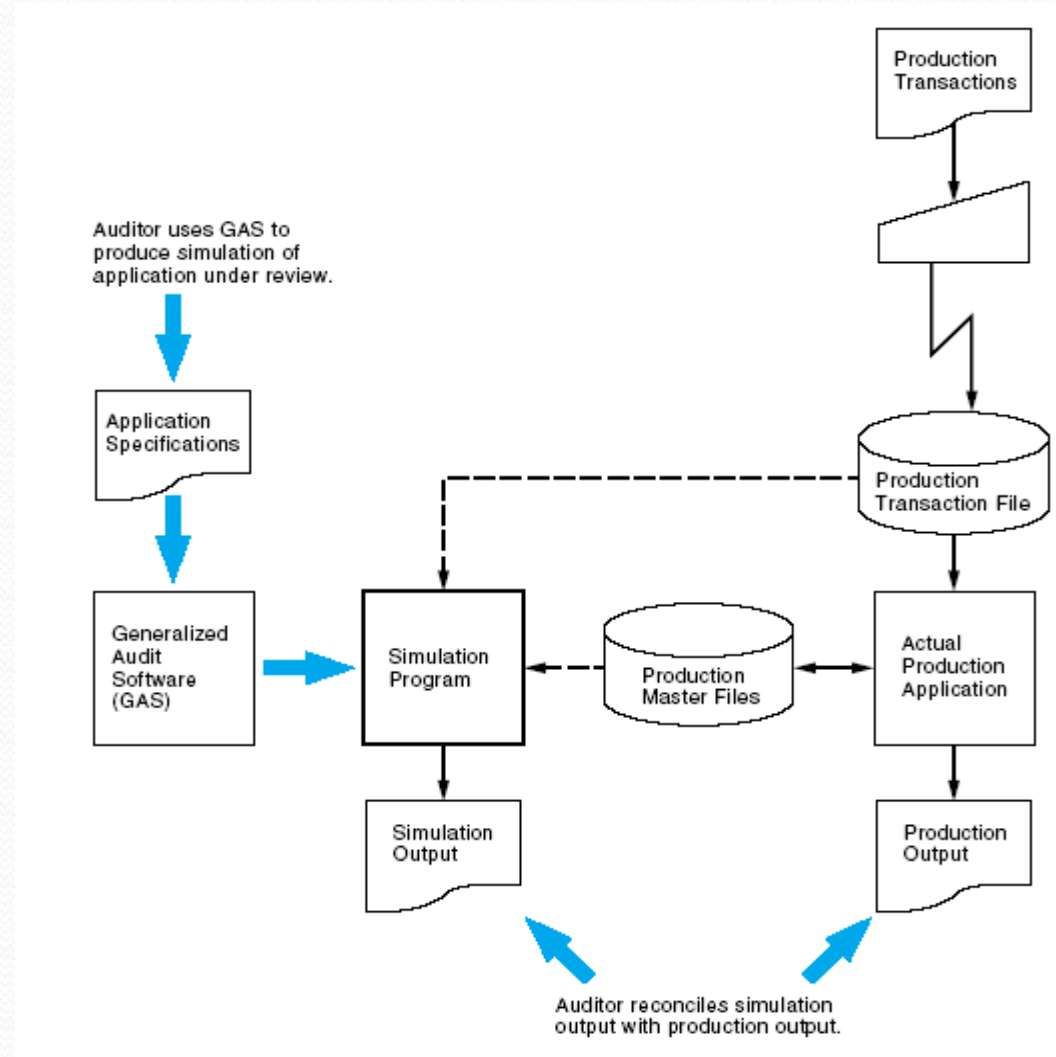
- **White Box Approach** - focuses on understanding the internal logic of processes between input and output
- Common tests
  - Authenticity tests
  - Accuracy tests
  - Completeness tests
  - Redundancy tests
  - Access tests
  - Audit trail tests
  - Rounding error tests



# White Box Testing Techniques

- **Test data method:** testing for logic or control problems - good for new systems or systems which have undergone recent maintenance
  - *base case system evaluation (BCSE)* - using a comprehensive set of test transactions
  - *tracing* - performs an electronic walkthrough of the application's internal logic
- Test data methods are not fool-proof
  - a snapshot - one point in time examination
  - high-cost of developing adequate test data

# Auditing through the Computer: The Parallel Simulation Technique



# Embedded Audit Module

- An ongoing module which filters out non-material transactions
- The chosen, material transactions are used for sampling in substantive tests
- Requires additional computing resources by the client
- Hard to maintain in systems with high maintenance



# Generalized Audit Software

- Very popular & widely used
- Can access data files & perform operations on them:
  - screen data
  - statistical sampling methods
  - foot & balance
  - format reports
  - compare files and fields
  - recalculate data fields