

The Management Control Framework – II

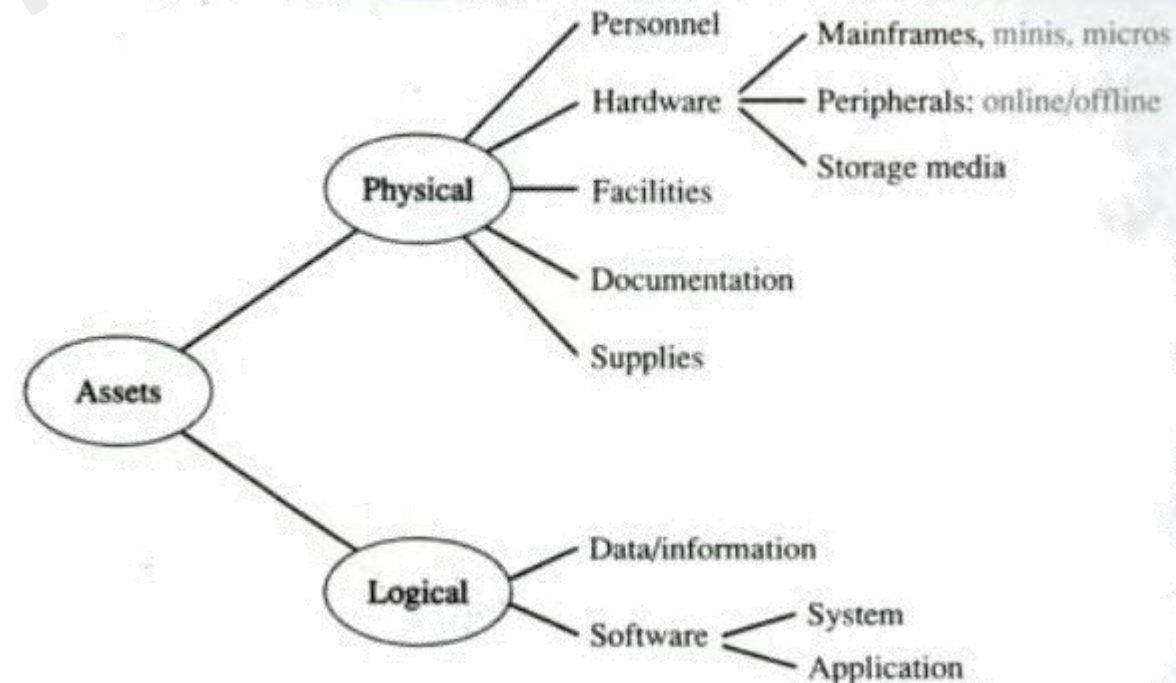
Dr. Jyotismita Chaki

Security Management Control

Security Management Control

- Assets are secure when the expected losses that will occur from threats eventuating over some time period are at an acceptable level.
- Three important aspects of this definition of security.
 - First, we accept that some losses will inevitably occur.
 - Second, we specify some level of acceptable losses.
 - Third, we must choose a time period.
- Classified in two ways (Figure 7-1).
 - The physical assets.
 - The logical assets.

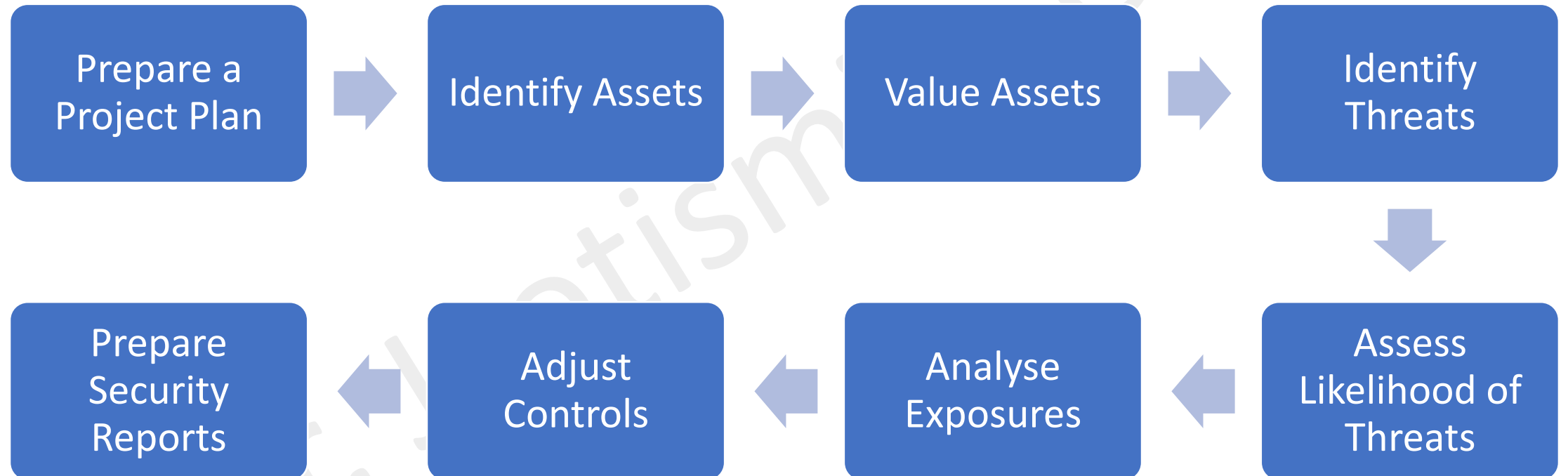
FIGURE 7-1. Categories of information systems assets.



Conducting a Security Programme

- Security administrators have to consider an extensive list of possible threats to the assets associated with the information systems function, prepare an inventory of assets, evaluate the adequacy of controls over assets, and perhaps modify existing controls or implement new controls.
- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews.
- If the security of information systems assets is at risk, asset safeguarding and data integrity objectives can be undermined.
- Similarly, system effectiveness and efficiency objectives can be undermined.
- The following slides describe eight major steps to be undertaken when conducting a security review
 1. preparation of a project plan,
 2. identification of assets,
 3. valuation of assets,
 4. threats identification,
 5. threats likelihood assessment,
 6. exposures analysis,
 7. controls adjustment, and
 8. report preparation.

Conducting a Security Programme



Conducting a Security Programme (Preparation of a Project Plan)

- The project plan for a security review should encompass the following items:
 - Objectives of the review: The objectives of the security review can be broadly based or narrowly defined.
 - Scope of the review: Defining scope is especially important, however, if the information systems function is widely dispersed throughout an organization.
 - Tasks to be accomplished: Although the overall tasks to be undertaken will be known, specific tasks must be defined.
 - Organization of the project team: The security administrator enlist the assistance of consultants or staff who have detailed knowledge of the areas to be evaluated.
 - Resources budget: It must specify the labor hours, materials, and money required to complete the review.
 - Schedule for task completion: The plan must specify which tasks must be completed by what dates.

Conducting a Security Programme (Identification of Assets)

- One way to identify assets is to seek out instances within various general categories.

<i>Asset Category</i>	<i>Examples</i>
Personnel	End users, analysts, programmers, operators, clerks, guards.
Hardware	Mainframe computers, minicomputers, microcomputers, disks, printers, communications lines, concentrators, terminals.
Facilities	Furniture, office space, computer rooms, tape storage racks.
Documentation	Systems and program documentation, database documentation, standards, plans, insurance policies, contracts.
Supplies	Negotiable instruments, preprinted forms, paper, tapes, cassettes.
Data/information	Master files, transactions files, archival files.
Applications software	Debtors, creditors, payroll, bill-of-materials, sales, inventory.
Systems software	Compilers, utilities, database management systems, operating systems, communications software, spreadsheets.

Conducting a Security Programme (Valuation of Assets)

- The valuation might differ depending on
 - Who values the asset: an asset might be more useful to some people than to others
 - How the asset is lost: accidental loss might be less serious than loss that arises through an irregularity
 - The time period of loss: for most assets the loss becomes more serious as use of the asset is denied for a longer period.
 - The age of the asset: most assets deteriorate with age.
- Valuation of physical assets also cannot be considered in isolation from valuation of logical assets.
- The primary objectives of asset valuation are to develop users' sensitivity to the possible consequences of a threat that eventuates and ultimately to enable an estimate to be made of the amount that can be justified as expenditure on safeguards.

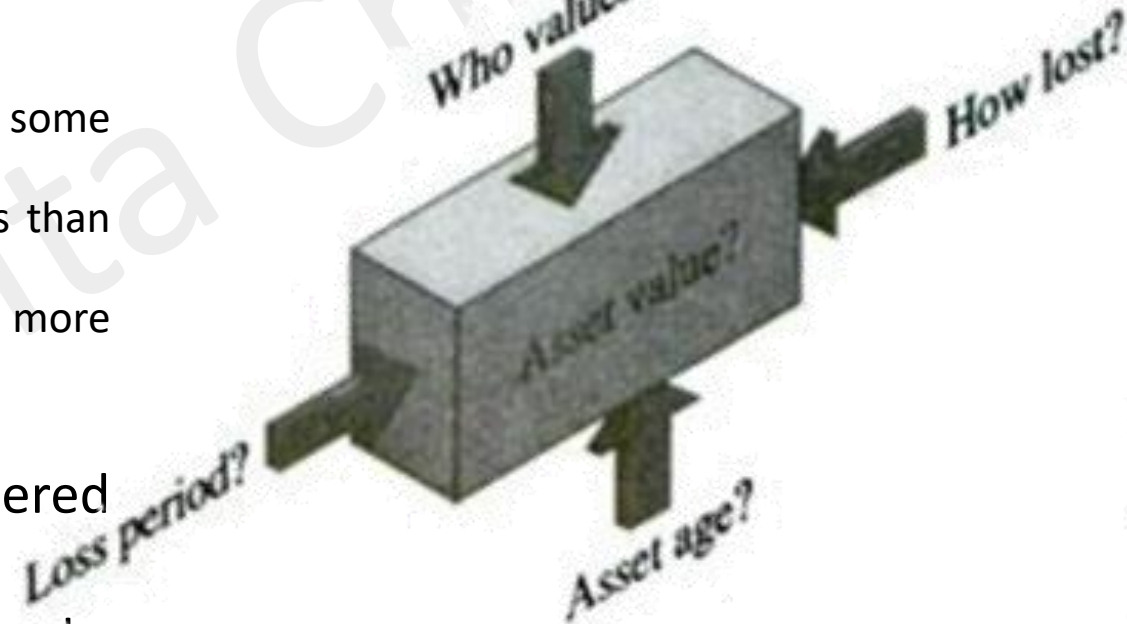


Figure: Factors that affect the valuation of the information systems assets

Conducting a Security Programme (Threats Identification)

- A threat is some action or event that can lead to a loss.
- During the threats identification phase, security administrators attempt to flesh out all material threats that can eventuate and generates results.
- One useful way to identify threats is first to consider possible sources of threats and then to consider the types of threats these sources might initiate

		Nature of threat	
		Accidental	Deliberate
Source of threat	External	e.g., Acts of God	e.g., Hackers
	Internal	e.g., Pollution	e.g., Sabotage

Figure: Types of threats facing information systems assets

Conducting a Security Programme (Threats Identification)

- The following threats arise from sources that are external to the organization

Source of Threat	Examples of Threat Types
Nature/Acts of God	Earthquake, flood, fire, mud, gases, projectiles, living organisms, extreme temperatures, electromagnetic Radiation
Hardware suppliers	Unreliable hardware, ineffective hardware, incompatible hardware, improper maintenance, lawsuits.
Software suppliers	Erroneous software, ineffective software, poor documentation, improper maintenance, lawsuits
Contractors	Erroneous software, ineffective software, improper hardware/software maintenance, untimely provision of services, disclosure of confidential information.
Other resource suppliers	Power outages, disruption to communication services, untimely provision of resources.
Competitors	Sabotage, espionage, lawsuits, financial distress through fair or unfair competition.
Criminals/Hackers	Theft, sabotage, espionage, extortion.

Conducting a Security Programme (Threats Identification)

- The following threats arise from sources that are internal to the organization

Source of Threat	Examples of Threat Types
Management	Failure to provide resources, inadequate planning and control.
Employees	Errors, theft, fraud, sabotage, extortion, improper use of services.
Unreliable systems	Hardware failure, software failure, facilities failure.

Conducting a Security Programme (Threats Likelihood Assessment)

- Security administrators must next attempt to estimate their likelihood of occurrence of each threat over a specified time period.
- In some cases, statistical data might be available.
- Often prior data is not available. Security administrators must then select the likelihood of occurrence of a threat from the stakeholders associated with an information system.
- Security administrators can use formal elicitation techniques to obtain estimates of the likelihood of occurrence of a threat.
- The identification and valuation of assets also assists with the identification of threats and their likelihood of occurrence
- Periodically, we must reassess the likelihood of a threat occurring.

Conducting a Security Programme (Exposure Analysis)

- Exposures arise because either
 1. There is no control to cover the threat incident or
 2. There is some probability that the control in place will not operate reliably for the particular threat incident that occurs
- Comprises four tasks:
 1. Identification of the controls in place;
 - use one of the many surveys designed to assess security
 2. Assessment of the reliability of the controls in place;
 - Straightforward Test: determine whether locked doors prevent unauthorized access to a computer room
 - Difficult Test: check whether fire extinguishers work
 3. Evaluation of the likelihood that a threat incident will be successful, given the set of controls in place and their reliability; and
 - Security administrators evaluate the probability of the control operating effectively to eliminate the effects of the threat incident
 - Security administrators write scenarios to describe how threat incidents could compromise controls
 4. Assessment of the loss that will result if a threat incident circumvents the controls in place.
 - The effect of the threat incident should first be determined
 - A value must be assigned to the effect
 - Security administrators must determine whether the full value of the asset will be lost if the threat is successful or whether the loss will be partial.

Conducting a Security Programme (Controls Adjustment)

- The benefits of a control that arise because it reduces expected losses from threats must exceed the costs of designing, implementing, and operating the control
- Guidance can be obtained from the control surveys used to identify missing controls during the exposures-analysis phase.
- Security administrators also might consult their colleagues in other organizations to determine control profiles that are used commonly
- Security administrators must examine whether existing controls should be terminated or modified in some way to improve their cost effectiveness.

Conducting a Security Programme (Report Preparation)

- This report documents the findings of the review and, in particular, makes recommendations as to new safeguards that should be implemented and existing safeguards that should be terminated or modified.
- The security report also must include a plan for implementing the safeguards recommended.

Operations Management Control

Introduction

- Responsible for the daily running of hardware and software facilities so that
 1. Production application systems can accomplish their work and
 2. Development staff can design, implement, and maintain application systems.
- In the late 1980s and early 1990s, four major changes occurred to the operations function from an auditor's perspective:
 1. Many operations tasks were automated.
 2. In many organizations the operations function became increasingly decentralized.
 3. Conflicting pressures emerged with respect to operations efficiency.
 4. Many organizations began to outsource their operations function.
- As a result, auditors became increasingly concerned about the control implications of contractual agreements with third parties

Responsibilities of Operations Management: Control

- Following are the controls that should exist over eight functions that are the responsibilities of operations management:
 1. Computer Operations
 2. Communication Network Control
 3. Data Preparation and Entry
 4. Production Control

Control: Computer Operations

- Three types of controls must exist:
 1. Operation Control: Those that prescribe the functions that either human operators or automated operations facilities must perform,
 2. Scheduling Control: Those that prescribe how jobs are to be scheduled on a hardware/software platform, and
 3. Maintenance Control: Those that prescribe how hardware is to be maintained in good operating order.

Computer Operations: Operations Control

- For an automated system, the following sorts of questions must be addressed by the auditors:
 1. Who authorizes the design, implementation, and maintenance of Automated Operations Facility (AOF) parameters?
 2. Are there standards to guide the design, implementation, and maintenance of AOF parameters?
 3. Are AOF parameters maintained in a secure file?
 4. How are new or modified AOF parameters tested?
 5. Is there ongoing monitoring of the authenticity, accuracy, and completeness of AOF operations?
 6. How well are AOF parameters documented?
 7. Is an up-to-date copy of AOF parameters stored off site?
- Auditors' evaluation of operations controls is further complicated by the diversity of hardware/software platforms encountered and the extensive decentralization of the operations function that has occurred in many organizations.
- Auditors must consider the need for operations controls across all hardware/software platforms.
- The diversity of audit approaches needed, where there is decentralization on the operations function.
- To collect evidence on the quality of operations controls, auditors can examine documentation, undertake interviews, and make observations.

Computer Operations: Scheduling Control

- The purpose of the schedule is to authorize use of hardware and system software resources by application systems.
- An operating system will provide an audit trails of job executed on a machine, and this audit trail can then be checked against the authorized schedule.
- Auditors should check for the existence of and enforcement of a production schedule.
- The auditor should expand substantive testing to determine, for example, whether users are satisfied with application systems and whether various types of machine resources have high utilization rates.
- Auditors must expand substantive testing if they assess control risk relating to production scheduling to be high.

Computer Operations: Maintenance Control

- Two types of maintenance of computer h/w
 - Preventive: undertaken to avoid h/w failure in the first place
 - Remedial: occurs on demand when h/w components no longer function properly
- In a mainframe and minicomputer environment, performance monitoring software should be used to prepare regular reports on hardware reliability.
- The operations manager should also review maintenance reports prepared by maintenance engineers to evaluate whether the levels of preventive and repair maintenance being undertaken are at acceptable levels.
- Maintenance engineers also might be required to sign a nondisclosure agreement in the event that sensitive data is exposed in the normal course of duties.
- Management can carry out background checking to assess the likely integrity of engineers.
- An auditor's primary concerns about hardware maintenance relate to effectiveness and efficiency objectives.
- auditors can interview the operations manager, engineers, and operators to determine what maintenance activities are performed and how.
- Auditors can examine documentation such as maintenance reports and logs

Network Operations: Wide Area Network Controls

- A network control terminal (important tool that operators use to manage a wide area network) provides access to specialized systems software that allows the following types of functions to be performed:
 - 1. Starting and stopping lines and processes,
 - 2. Monitoring network activity levels,
 - 3. Renaming communications lines,
 - 4. Generating system statistics,
 - 5. Resetting queue lengths,
 - 6. Increasing backup frequency,
 - 7. Inquiring as to system status,
 - 8. Transmitting system warning and status messages, and
 - 9. Examining data traversing a communications line.

Network Operations: Wide Area Network Controls

- Several controls must be exercised over operator use of a network control terminal:
 1. Only senior operators who are well trained and have a sound employment history should perform network control functions.
 2. To the extent possible, network control functions should be separated and duties rotated on a regular basis.
 3. The network control software must allow access controls to be enforced so that each operator is restricted to performing only certain functions.
 4. The network control software must maintain a secure audit trail of all operator activities.
 5. Operations management must regularly review the audit trail to determine whether unauthorized network operator activities have occurred.
 6. If multiple network control terminals are used, network control functions should be partitioned and restricted to a particular terminal.
 7. Documented standards and protocols must exist for network operators.
 8. Operations management must regularly review network operator activities for compliance with standards and protocols

Network Operations: Wide Area Network Controls

- Auditors can evaluate the reliability of controls over the operations of wide area networks using interviews, observations, and review of documentation
- They can observe network operators as they carry out their work
- They can review reports prepared on the basis of network control terminal logs

Network Operations: Local Area Network Controls

- Operations management of local area networks occurs via the facilities provided on file servers.
- A file server plays an important role in supporting the access control mechanisms used in a local area network such as
 - Available disk space on a file server can be monitored.
 - Utilization activity and traffic patterns within the network can be monitored.
 - Levels of corrupted data within the network can be monitored.
 - Special network cards are often employed to connect workstations to a local area network.
 - A file server can be used to execute software that prevents, detects, and removes viruses.
- Auditors can use interviews, observations, and reviews of documentation to evaluate the reliability of controls over the operations of local area networks.
- The auditor can observe whether file servers are located in a secure area and whether access to file servers appears to be restricted to authorized personnel.

Data Preparation and Entry

- Some types of data preparation and entry equipment require regular maintenance.
- Operations management must ensure that backup exists for both input data and data preparation and entry devices.
- Data entered directly into computer systems (no source documents) should be backed up as part of the normal file backup system.
- Auditors should enquire whether an organization has a set of standards to govern data preparation and entry activities.
- Weak controls over data preparation and entry can have a fairly direct impact on the four objectives of asset safeguarding, data integrity, system effectiveness, and system efficiency.

Production Control

- The production control section under operations management performs five major functions:
 - (1) receipt and dispatch of input and output,
 - (2) job scheduling.
 - (3) management of service-level agreements with users,
 - (4) transfer pricing/chargeout control, and
 - (5) acquisition of computer consumables.
- production control personnel are responsible for receipt of and dispatch of output to outside parties and users.
 - First, they might need to ensure that output is prepared on a timely basis.
 - Second, production control personnel might perform some types of basic quality assurance checks on any output received on behalf of outside parties or users.
 - Third, production control personnel might be responsible for safe custody of product and dispatch of output.

Quality Assurance Management Control

Introduction and Motivation

- Quality Assurance (QA) Management is concerned with ensuring:
 1. The information system produced by the information system function achieve certain quality goals.
 2. Development, implementation, operation, and maintenance of information systems comply with a set of quality standards.
- There are six reasons why the information systems QA Role has emerged in many organization
 - safety critical information systems
 - Demanding users
 - ambitious projects
 - Organizations concerned about their liabilities
 - Poor quality control over the production, implementation, operation, and maintenance of software
 - Poor quality control over the production, implementation, operation, and maintenance of software

QA Functions

- Information system personnel perform a monitoring role for management to ensure that:
 1. Quality goals are established and understood clearly by all stakeholders
 2. Compliance occurs with the standards that are in place to attain quality information systems

QA Functions

- Six specific functions that QA personnel should perform.
 - Developing Quality Goals
 - Developing, Promulgating and Maintaining for the Information System Function
 - Monitoring Compliance with QA Standards
 - Identifying Areas for Improvement
 - Reporting to Management
 - Training in QA Standards and Procedures

Organizational Considerations Placement of the QA function

- Auditors can interview QA staff, information systems staff, and information system users to determine the scope and depth of QA work and to assess whether funding of the QA function
- Staffing the QA function
- Relationship between Quality Assurance and Auditing: Objectives and Functions of QA personnel and auditors are the same.

The Application Control Framework

Dr. Jyotismita Chaki

Introduction

- Application controls are transactions and data relating to each computer-based application system and are specific to each application.
- Objectives – ensure that:
 - Input data is accurate, complete, authorized, and correct.
 - Data is processed as intended in an acceptable time period.
 - Data stored is accurate and complete.
 - Outputs are accurate and complete.
 - A record is maintained to track the process of data from input to storage and to the eventual output.

Types

- Input control
 - Input authorization
 - Batch controls and balancing
 - Error reporting and handling
- Processing control
 - Data validation and editing procedures
 - Processing controls
 - Data file control procedures
- Output control
 - Where the sensitive report was printed?
 - Was distribution controlled?
 - How long are the sensitive reports retained?
 - Are they stored in a protected environment?
 - Are they protected from disclosure, or, are they confidential?

Benefits

- Reliability
 - Application controls are more reliable than manual controls when evaluating the potential for control errors due to human intervention.
 - Application control will continue to operate effectively if the information technology general controls that have a direct impact on its programmatic nature are operating effectively as well.
- Time and Cost Savings
 - Application controls typically take less time to test than manual controls.
 - Application controls are typically tested one time, as long as the information technology general controls are effective.

Benefits

- Benchmarking

- The auditor should evaluate the appropriate use of benchmarking of an automated control by considering how frequently the application changes.
- benchmarking is particularly effective when companies use pre-packaged software that doesn't allow for any source code development or modification.
- Once the benchmark is no longer effective, it is important to re-establish the baseline by re-testing the application control.
- Auditors should ask:
 - Have there been changes in the risk level associated with the business process and the application control from when it was originally benchmarked?
 - Are ITGCs operating effectively, including logical access, change management, systems development, acquisition, and computer operation controls?
 - Can the auditor gain a complete understanding of the effects of changes, if any, on the applications, databases, or supporting technology that contain the application controls?
 - Were changes implemented to the business process relying on the application control that could impact the design of the control or its effectiveness?

Role of internal auditors: Input control checklist

1. Are there training policies and processes for data preparation and input personnel?
 - a) Are training activities adequate for new personnel and are there any regular training programs?
 - b) Is there a regular training program to update users on new applications?
 - c) If a user's manual or written procedures exist for the preparation, handling and input of data for the application under study, do they accurately reflect current practice?

Role of internal auditors: Input control checklist

2. Review and evaluate the design of the key source documents.
 - a) Are source documents designed in a manner that facilitates the initial recording of data in a uniform, complete, and accurate format?
 - b) Are source documents serially pre-numbered with a cross-reference number (such as a receipt #, check #) to serve as an audit trail and to facilitate tracing to/from computerized reports?
 - c) Do source documents provide a unique code or identifier for each transaction type to provide an audit trail?
3. Evaluate and review the procedures involved in the handling of blank source documents.
 - a) Are blank source documents stored in a secure location and in the custody of designated persons who have no role in their preparation?
 - b) Is the release of blank source documents from storage adequately controlled through the use of logs and proper authorizations?

Role of internal auditors: Input control checklist

4. Is there a preprocessing review of source documents prior to data input to detect errors in completeness and consistency as well as obvious mistakes?
 - a) Is there a preprocessing review of source documents performed by someone other than the preparer?
 - b) If source documents are maintained on-line, are controls in place to ensure review of the documents on-line?

Role of internal auditors: Input control checklist

5. Evaluate and review the transaction approval process of the key source documents
 - a) Are all source documents approved by someone other than the preparer?
 - b) Is evidence of approval required for all transactions (or only for critical ones)?
 - c) Determine whether the system generates summary (or detail) reports showing the transaction types input and approved for each user. Is this report reviewed by management?
 - d) Is there any physical evidence to verify that the review was performed?
 - For manual Input:
 - e) Are signatures compared to a list of authorized signers in order to verify proper source document approval?
 - f) Are any methods other than signatures or initials used to provide evidence of approval?

Role of internal auditors: Input control checklist

5. Evaluate and review the transaction approval process of the key source documents

- Online approval

- g) Are users given the appropriate approval authority?
- h) Are users restricted from approving a transaction which they initiated?
- i) Are all documents (screens) approved?

Role of internal auditors: Input control checklist

6. Determine whether the controls in effect are sufficient to account for all transactions.

- For batch input

- a) Are source documents batched in manageable groups of similar transaction types?
- b) Are the batches assigned a unique sequential identification number?
- c) Are control totals used and compared at intervals during the processing?
- d) Are discrepancies resolved and documented?
- e) Does a batch header card accompany the batch throughout the input process and is it retained with the batch to serve as an audit trail?
- f) Are the batches logged-in and verified?

Role of internal auditors: Input control checklist

6. Determine whether the controls in effect are sufficient to account for all transactions.

- Online, Real time, Non batch input

- g) Does the system establish control totals such as by processing run, input time of day, specific input terminal, or individual inputting the data? Are control totals further computed by type of transaction?
- h) Are these control totals reconciled to control accounts by an independent supervisor?
- i) Are these control totals reconciled by the system and any differences reported and followed up by error control personnel?
- j) If the aforementioned controls are missing, are there compensating controls such as independent reconciliation of input source to control listings or other output reports?
- k) Do data entry operators stamp or otherwise mark batches or source documents once they have been input in order to prevent duplicate processing of transactions?

Role of internal auditors: Input control checklist

6. Determine whether the controls in effect are sufficient to account for all transactions.

- Other input

- l) Are magnetic tapes/cartridges delivered to the computer operations area controlled to ensure all data are processed?
- m) Are documents delivered to the computer operations area for scanning or imaging controlled to ensure all data are processed?
- n) Are inbound Electronic Data Interchange (EDI) transactions written to a file and logged to establish input control prior to being processed by the application system?
- o) Are other types of input methods controlled to ensure all data are processed?

Role of internal auditors: Input control checklist

7. Examine the process and controls over error detection, correction, and reentry of transactions.
 - a) Are there procedures over the detection, correction, and reentry of errors?
 - b) If on-line system input techniques are used, skip to 8c. In batch systems, are controls over the delivery of the rejected batches proper to ensure that they are not lost?
 - c) Are data entry operators in on-line systems restricted from making corrections of any non-keying errors?
 - d) Are error messages maintained on-line or on the error exception reports clear and easily understood so that the proper corrective actions may be taken?
 - e) Are error exception reports corrected, dated, and retained for management review?
 - f) Are corrected errors reviewed and approved by management before reentry?

Role of internal auditors: Process control checklist

1. Review the controls that ensure all input transactions are processed by the computer
 - a) Are record counts and control totals verified to ensure that all data are processed?
 - b) Is there evidence (audit trail) of transactions processed/rejected being reconciled or investigated?

Role of internal auditors: Process control checklist

2. Determine the critical edits and checks necessary for each application. Critical edits and checks should consist of some or most of the following types. Do such edits and checks include:
 - a) A reasonableness check which determines if an amount or date is greater or less than a predefined limit?
 - b) A dependency edit which verifies the expected relationship of one field to another?
 - c) A sequence check which is used to detect missing document numbers?
 - d) A duplicate number check?
 - e) An existence edit which determines whether the transaction data matches data on file or look-up tables?
 - f) A format edit which could be used to make sure only numeric data is included in numeric fields or alpha data in alpha-only fields?
 - g) A mathematical check to foot and cross-foot all applicable amount fields?
 - h) A range check which could be utilized to test whether data falls within certain pre-set ranges?
 - i) A confirmation check which utilizes stored data to confirm the modification of infrequently changed data? (An example would be transactions that alter values, such as pay rate changes.)

Role of internal auditors: Process control checklist

3. Do error handling procedures include:

- a) Are rejected transactions held in an error suspense file and/or prevented from updating the master files?
- b) Does the system prepare printouts listing all transactions held in the suspense file?
- c) Are entries in error suspense identified as to age and type?
- d) Are corrected transactions subjected to the same edit, review and approval controls that were applied to the original transaction?

4. If the application observed produces system-generated transactions (for instance, offsetting accounting entries), are they printed out and reviewed by the appropriate personnel?

Role of internal auditors: Output control checklist

1. Are current and accurate procedures for balancing and reconciling output formally documented?
2. Are output control totals compared and agreed to input and processing control totals?
3. Are output reports balanced and reconciled to output from related systems?
4. If user management receives and reviews the following reports,
 - a) Are detail or summary transaction reports scanned for unusual results?
 - b) Are reports of sensitive on-line master file updates (such as pay rate changes, employee status changes, vendor name changes, etc.) reviewed for unauthorized or erroneous modifications to sensitive information?
5. Are output distribution lists produced which show the reports that are generated for each application processing run?
6. Are output distribution logs maintained to record the date and/or time received and the signatures of the users authorized to receive the output?

Evidence Collection

Dr. Jyotismita Chaki

Introduction

- Audit evidence is all the information used by the auditor in arriving at the conclusions on which the audit opinion is based and includes the information contained in the IT records.
- Audit evidence, which is cumulative in nature, includes audit evidence obtained from audit procedures performed during the course of the audit and may include audit evidence obtained from other sources, such as previous audits and a firm's quality control procedures for client acceptance and continuance.

Introduction

- An auditor must gather sufficient and appropriate audit evidence and test them to make a judgment of opinion.
- In gathering evidence to support his assertions, the auditor is often confronted with two issues;
 - 1.What evidence will be relevant to assess an assertion with greater reliability?
 - 2.How much evidence is to be obtained?

Sufficient and appropriate audit evidence

- The auditor should design and perform audit procedures that are appropriate in the circumstance for the purpose of obtaining sufficient appropriate audit evidence.
- Appropriateness is the measure of the quality of audit evidence.
- The quantity of audit evidence needed is affected by the risk of misstatement and also by the quality of such audit evidence.

Ways of collecting audit evidence

Inspection

- Involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or a physical examination of an asset.
- Provides audit evidence of varying degrees of reliability, depending on their nature and source.

Observation

- consists of looking at a process or procedure being performed by others.
- provides audit evidence about the performance of a process or procedure but is limited to the point in time at which the observation takes place

External Confirmation

- represents audit evidence obtained by **the auditor** as a direct written response to the auditor from a third party (the confirming party), in paper form, or by electronic or another medium.

Interviews

- System analysts and programmers: better understanding of the functions and controls embedded within the system.
- Data entry staff: how they correct input data that the application system identifies as inaccurate or incomplete
- Users of an application system: their perceptions of how the system has affected the quality of their working life.
- Operations staff: whether any application system seem to consume abnormal amounts of resources when they are executed.

Questionnaires

- to flag areas of system weakness during evidence collection.
- to identify areas within an information system where potential inefficiencies exist
- Questions must be specific.
- Must be used a language which is understandable by the intended person.

Flowchart

- Comprehension – the construction of a control flowchart highlights those areas where auditors lack understanding of either the system itself or the controls in the system;
- Evaluation – experienced auditors can use control flowcharts to recognize patterns that manifest either control strengths or control weakness in a system;
- Communication – auditors can use control flowcharts to communicate their understanding of a system and its associated controls to others.

Analytical procedures

- use comparisons and relationships to determine whether information system appear reasonable.
- should be performed early in the audit to aid in deciding
 - which information system parts do not need further verification,
 - where other evidence can be reduced and
 - which audit areas should be more thoroughly investigated.

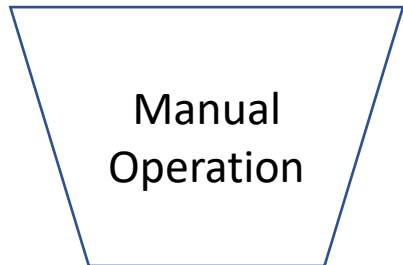
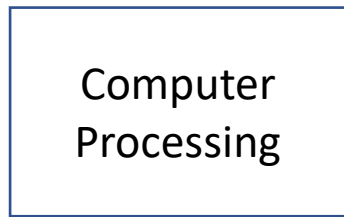
Documentation

- auditor's examination of the client's documents and records to substantiate the **information that is or should be included in the IT audit statements.**

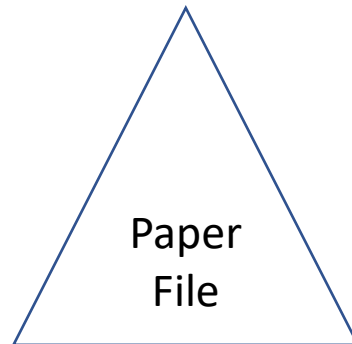
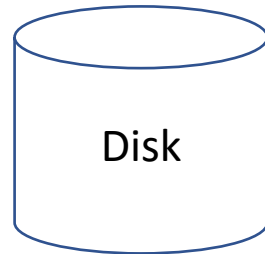
Document Flowchart

Subset of flowcharting symbol

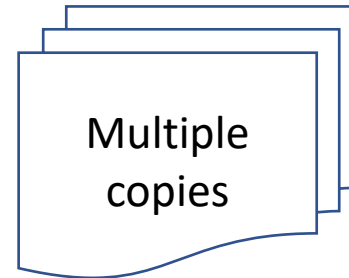
Processes



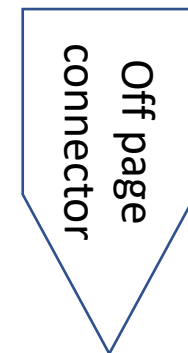
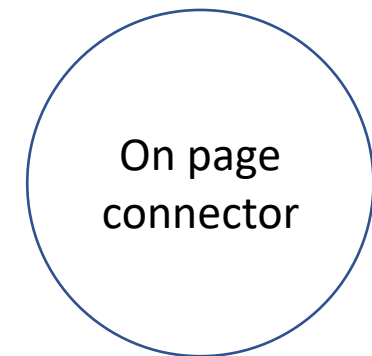
Storage Files



Input / Output



Miscellaneous



Introduction

- Document flowcharts have the purpose of showing existing controls over document-flow through the components of a system.
- These flowcharts are typified by their vertical structure.
- The chart is read from left to right and documents the flow of documents through the various business units.

Example

- ABC Appliances Ltd. is a popular marketing company which has many branches located in different places. With increased business activities, the company faces several problems with the existing information system. The company realizes that the existing information system is outdated and needs improvement. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts, and system designers. The team has executed all phases in SLDC and implemented the new system successfully. Requirement analysis is done by the project managers and prepares a requirement analysis report and forwards it to the system designers; design, implementation and testing are done by system designers based on the requirement analysis report and testing report is generated. Deployment and maintenance is done by system analyst based on the testing report and maintenance report is generated. Now the company has decided to engage the XYZ consultancy services to audit the system regularly. Every month, the auditor from XYZ consultancy services updates the audit report and forwards the report to the project manager.

Building step1: Identify external and internal agents

- ABC Appliances Ltd. is a popular marketing company which has many branches located in different places. With increased business activities, the company faces several problems with the existing information system. The company realizes that the existing information system is outdated and needs improvement. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts, and system designers. The team has executed all phases in SLDC and implemented the new system successfully. Requirement analysis is done by the project managers and prepares a requirement analysis report and forwards it to the system designers; design, implementation and testing are done by system designers based on the requirement analysis report and testing report is generated. Deployment and maintenance is done by system analyst based on the testing report and maintenance report is generated. Now the company has decided to engage the XYZ consultancy services to audit the system regularly. Every month, the auditor from XYZ consultancy services updates the audit report and forwards the report to the project manager.

Building step2: Identify processes

- Processes can include actions related to documents / reports and data stores (data entry, verification, classifications, arrangements, sorting, calculation, summarization, retrieving data)
- Processes do not include interaction with products.
- Include only normal processes, not exception processes, error processes, or control processes.
- Group similar or related processes for each internal agent.

Building step2: Identify processes

- ABC Appliances Ltd. is a popular marketing company which has many branches located in different places. With increased business activities, the company faces several problems with the existing information system. The company realizes that the existing information system is outdated and needs improvement. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts, and system designers. The team has executed all phases in SLDC and implemented the new system successfully. Requirement analysis is done by the project managers and prepares a requirement analysis report and forwards it to the system designers; design, implementation and testing are done by system designers based on the requirement analysis report and testing report is generated. Deployment and maintenance is done by system analyst based on the testing report and maintenance report is generated. Now the company has decided to engage the XYZ consultancy services to audit the system regularly. Every month, the auditor from XYZ consultancy services prepare the audit report and forwards the report to the project manager.

Building step3: Identify data store and table

- ABC Appliances Ltd. is a popular marketing company which has many branches located in different places. With increased business activities, the company faces several problems with the existing information system. The company realizes that the existing information system is outdated and needs improvement. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts, and system designers. The team has executed all phases in SLDC and implemented the new system successfully. Requirement analysis is done by the project managers and prepares a requirement analysis report and forwards it to the system designers; design, implementation and testing are done by system designers based on the requirement analysis report and testing report is generated. Deployment and maintenance is done by system analyst based on the testing report and maintenance report is generated. Now the company has decided to engage the XYZ consultancy services to audit the system regularly. Every month, the auditor from XYZ consultancy services prepare the audit report and forwards the report to the project manager.

Building step4: Draw a column for each agent

Project Manager

System Designer

System Analyst

IS Auditor

Dr. Jyotismita Chakraborty

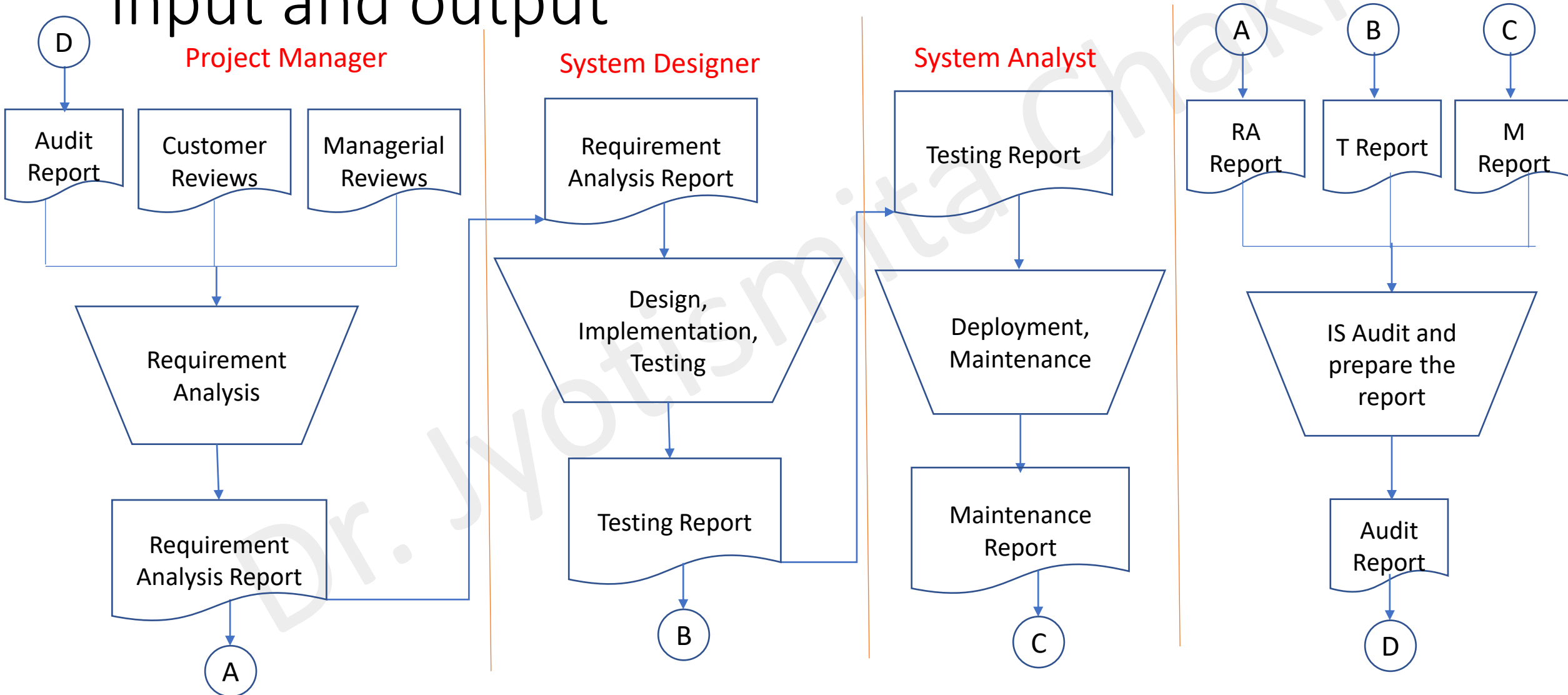
Building steps5: Draw processes and related input and output

IS Auditor

Project Manager

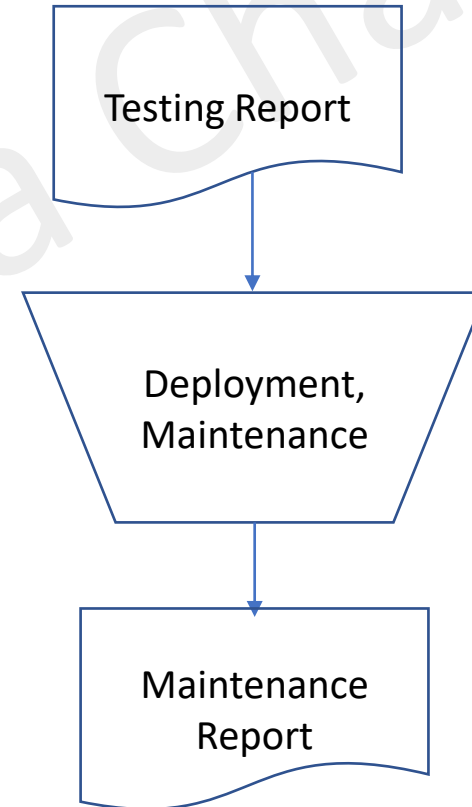
System Designer

System Analyst

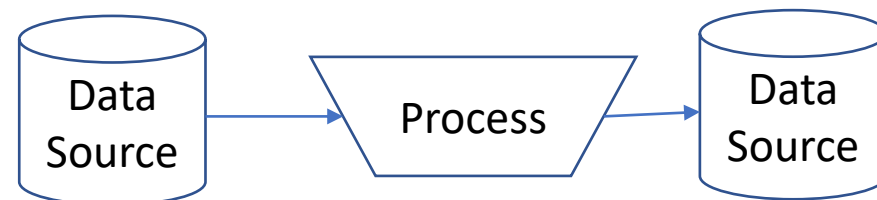
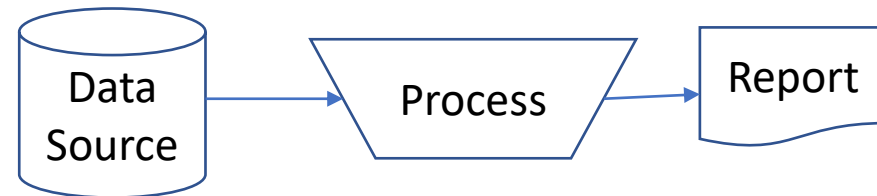
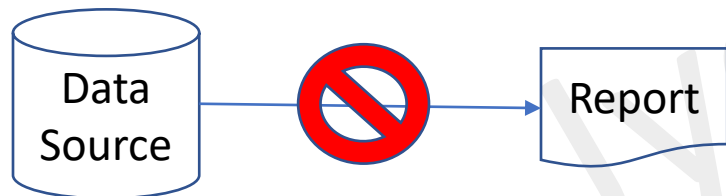
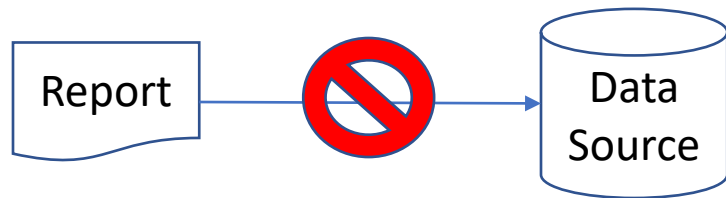
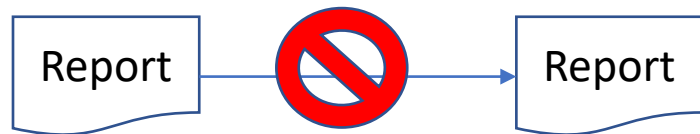


Important Tips

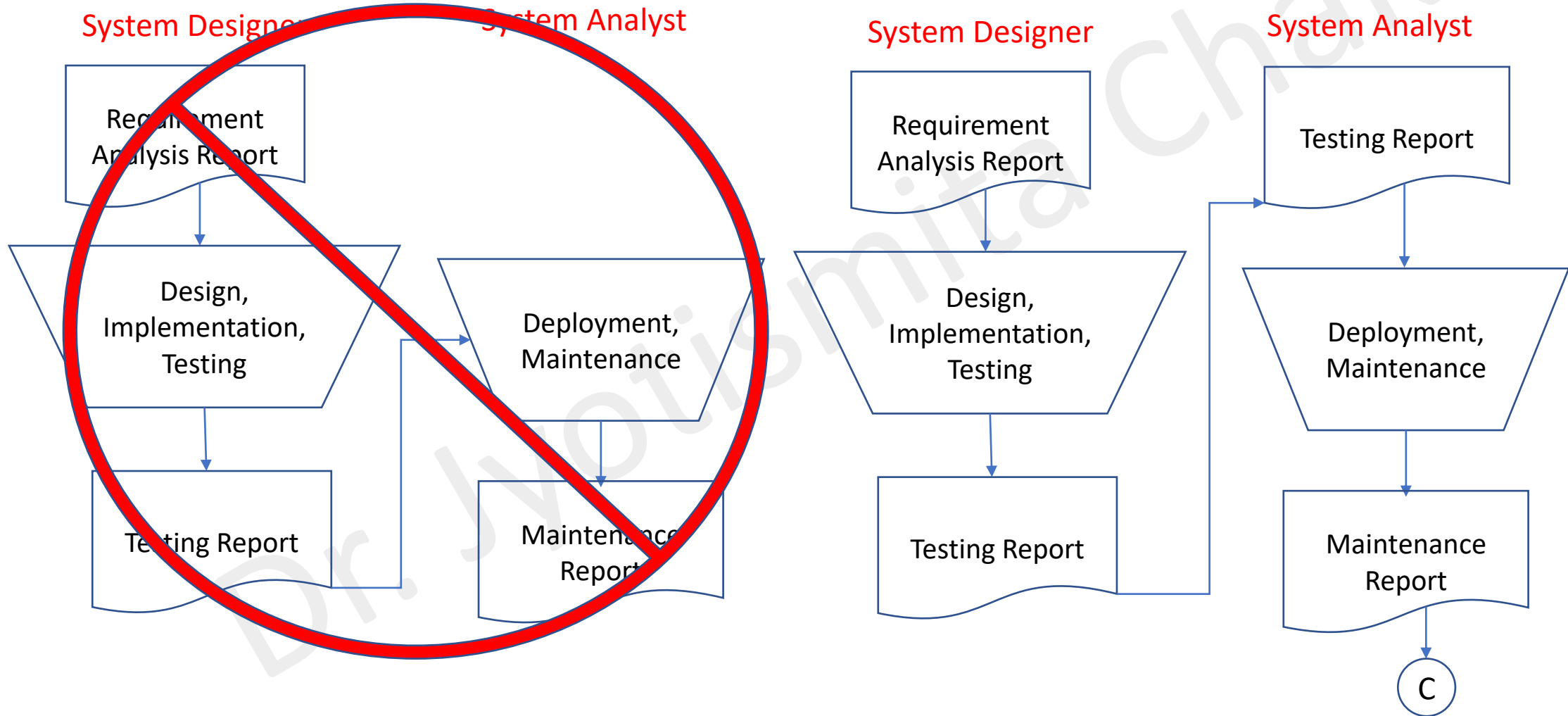
- Every process should have at least one input and one output



Important tips



Important tips

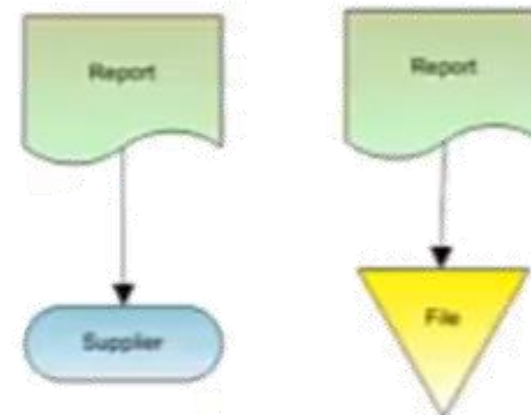
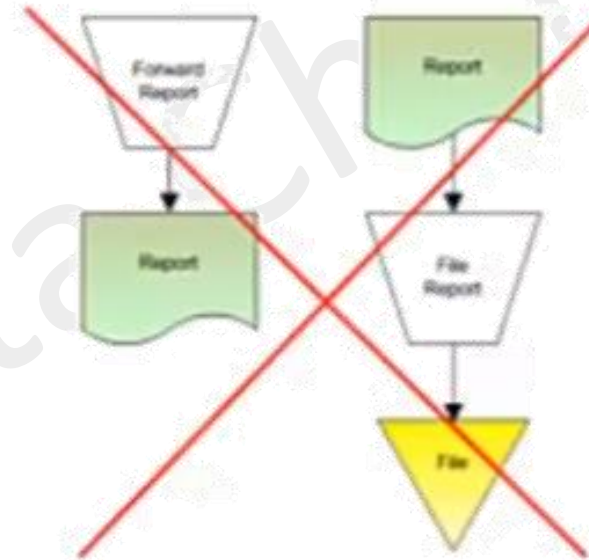


Show the same document in both locations

Important tips

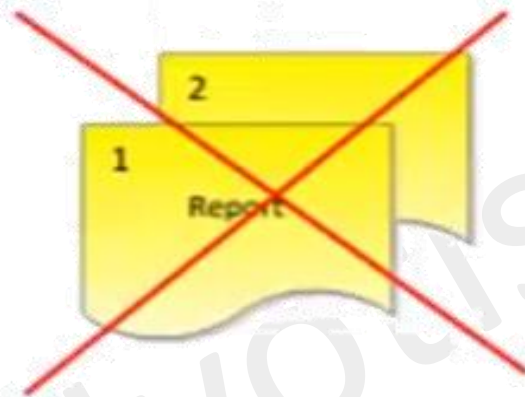
- Do not show process symbols for
 - Forwarding a document to another entity
 - Filing a document

- Show this instead →



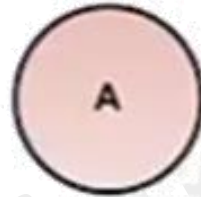
Important tips

When using multiple copies of a document, overlap the documents and place document numbers in the upper, right-hand corners.



Important tips

- **Show on-page connectors and label them clearly to avoid excess lines.**



- **Use off-page connectors when the flow goes to another page.**

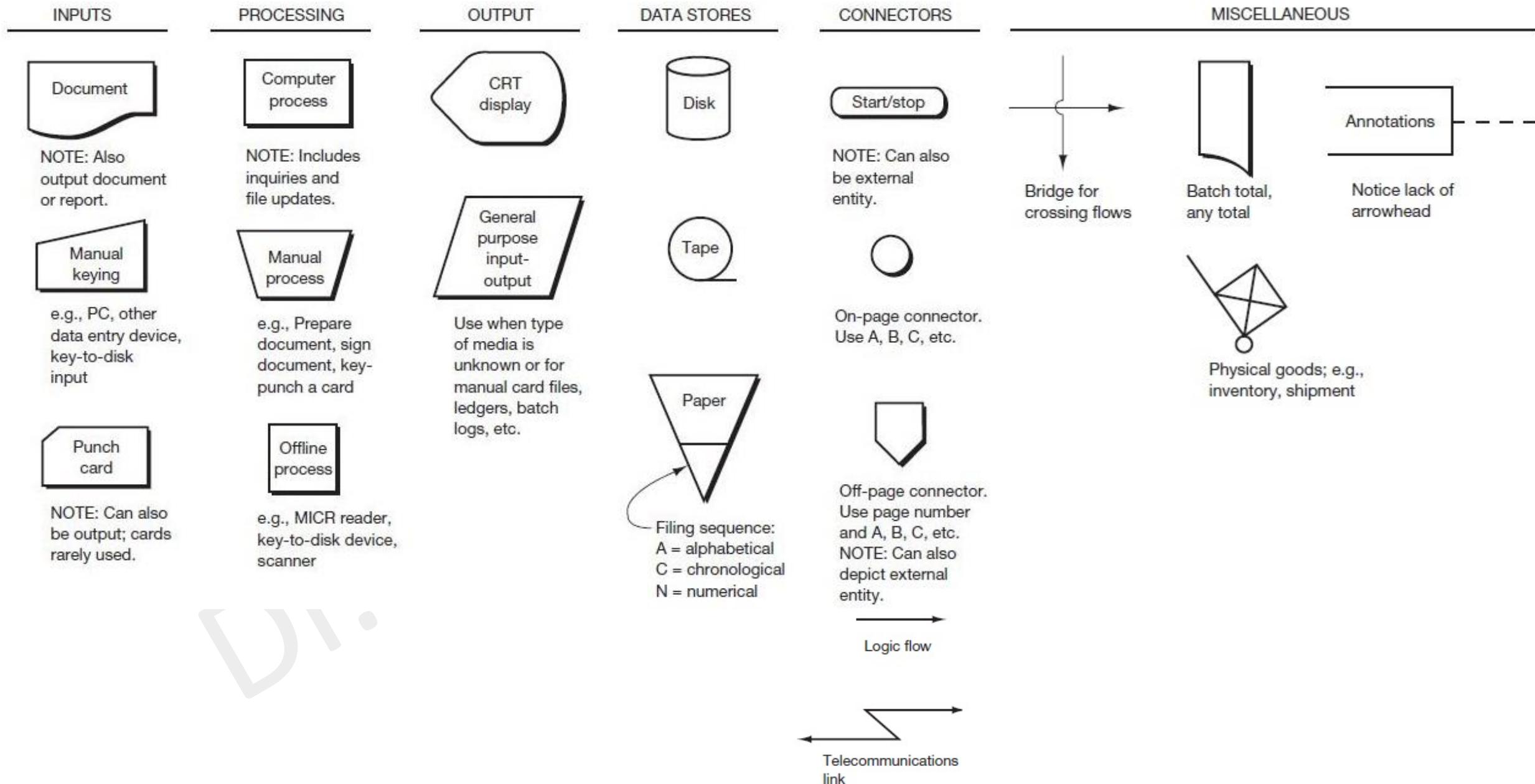


System Flowcharts

Introduction

- Graphical representation of *information processes* (activities, logic flows, inputs, outputs, and data storage), as well as the related *operations processes* (entities, physical flows, and operations activities).
- Includes both manual and computer activities, the systems flowchart presents a logical and physical rendering of the who, what, how, and where of business processes and Information Systems.
- Shows the flow of data to and through the major components of a system such as, data entry, programs, storage media, processors, and communication networks.
- These types of flowcharts demonstrate how the controls are placed to ensure the correct functioning of the named components

Subset of flowcharting symbol



Example1

- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.

Building step1: Identify the internal and external agents

- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.

Building step2: Identify input / output

- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.

Building step3: Identify processes

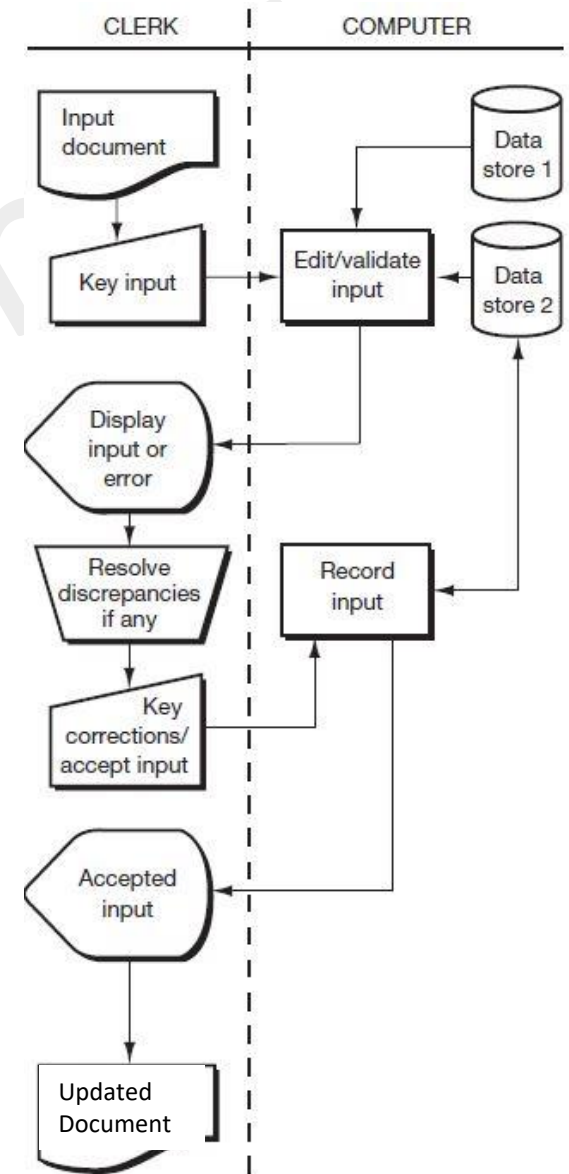
- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.

Building step4: Identify the data store

- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.

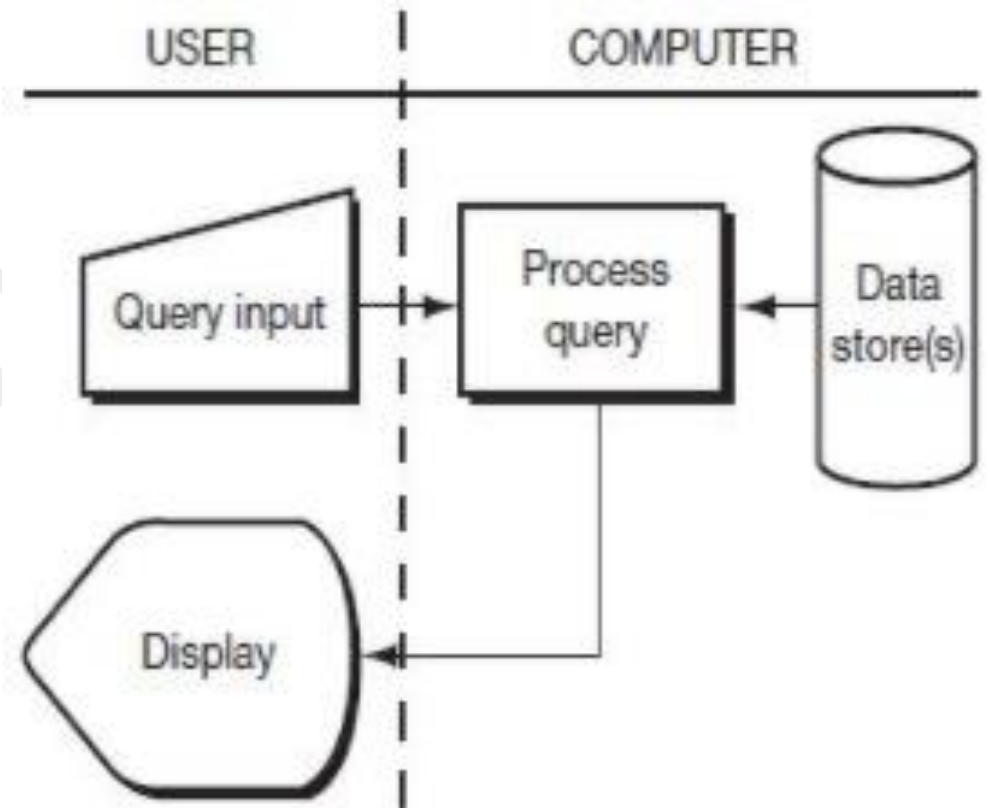
Building step4: Build the system flowchart

- The data entry clerk keys a sales input document while online. The computer accesses data in data store 1 (perhaps a table of valid codes, such as customer codes) and in data store 2 (perhaps a table of open sales orders) to edit/validate the input. The computer displays the input, including any errors. The clerk compares the input document to the display, keys in corrections as necessary, and accepts the input. The computer updates the table in data store 2 and notifies the clerk that the input has been recorded.



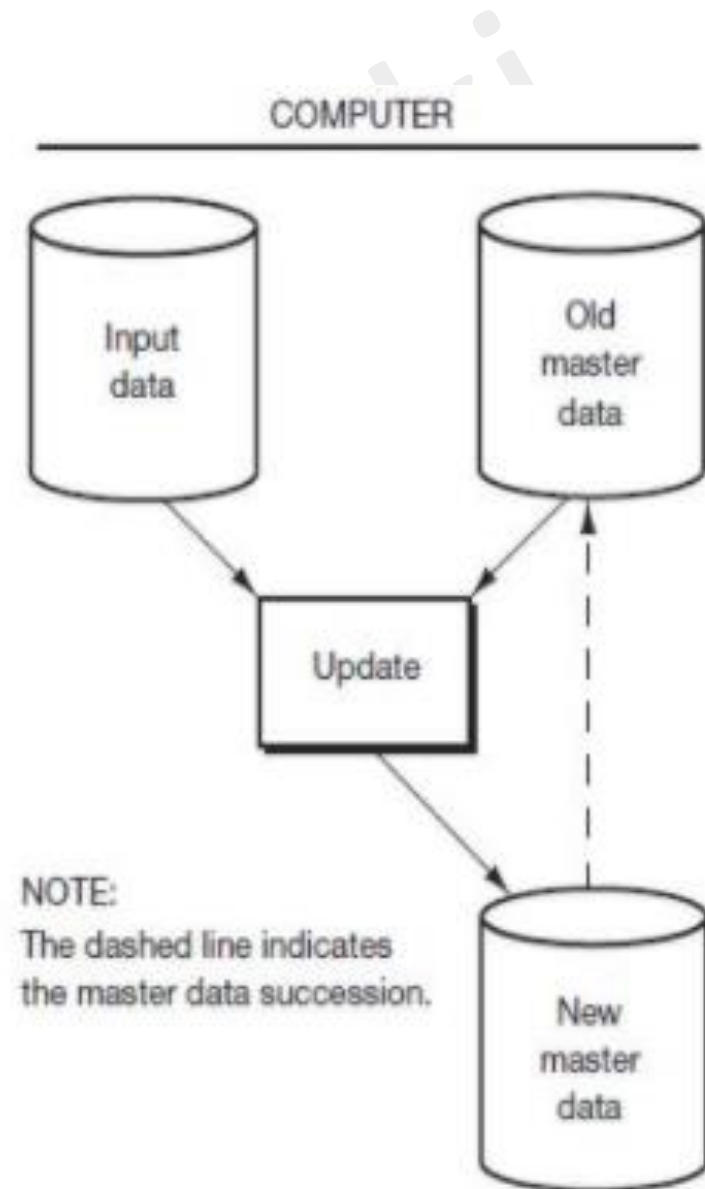
Example 2

- A user keys a query request online into a computer. The computer accesses the table(s) in one or more data stores and presents a response to the user.



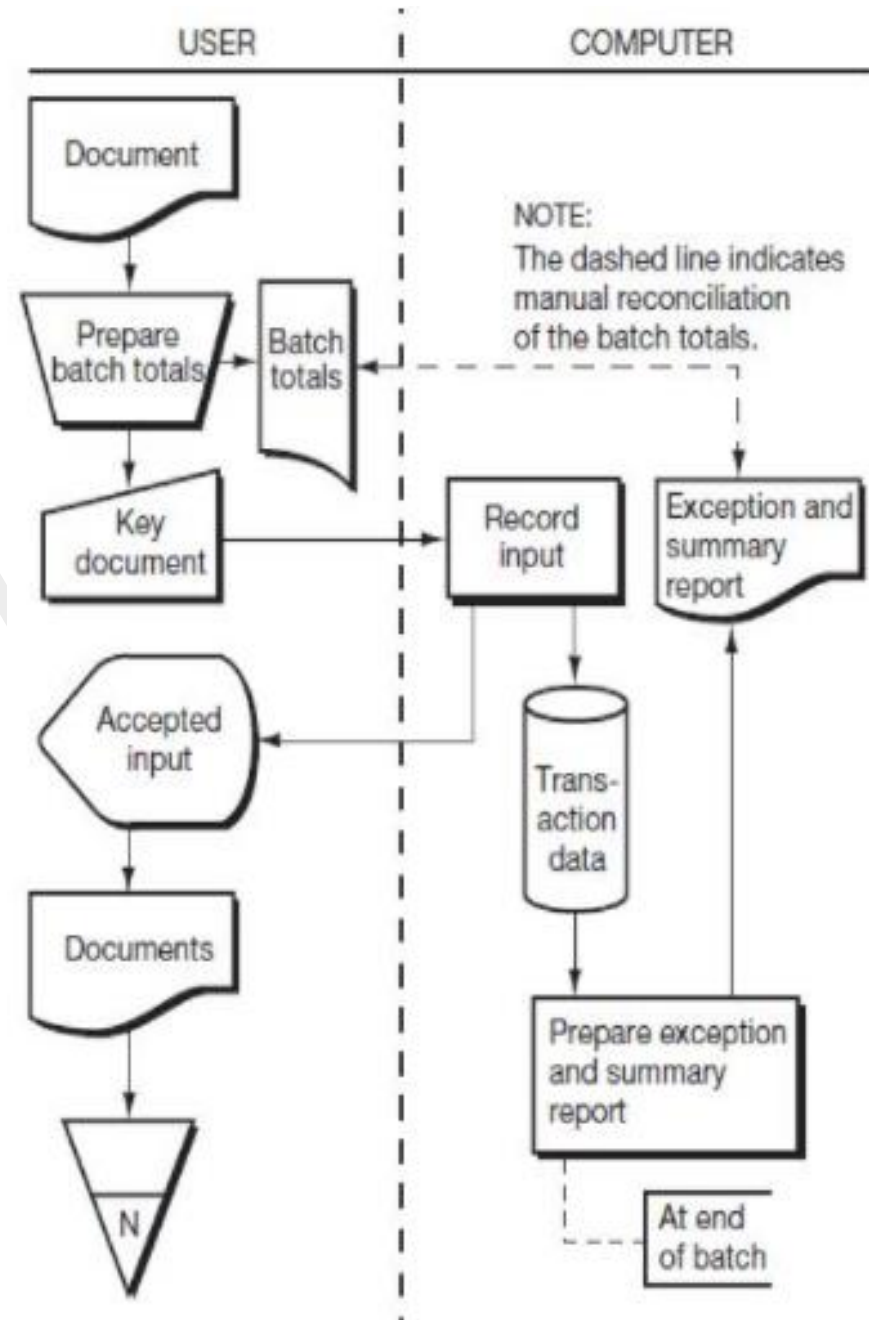
Example 3

- New data (a customer address change, for example) previously recorded on disk are input to the computer, along with the existing (old) master data (customer master data, for example). The computer updates the existing master data and creates a new version of the master data.
 - When sequential master data is updated, two data store symbols are used on a flowchart. One symbol represents the existing (old) version and the other represents the new version.
 - A dashed line connects the new with the old master data version to show that the new *becomes* the old version during the next update process.



Example 4

- The user collects a number of input documents in a “batch” (such as a week’s worth of time cards), prepares batch totals, and enters the documents into the computer. The computer records the inputs on a disk and notifies the user as each input is accepted. The user files the input documents in numerical sequence. At the end of the batch, the computer prepares an exception and summary report (a list of inputs accepted and rejected by the system) that includes batch totals. The user compares the computer batch totals to those prepared prior to entry of the documents to make sure the data were entered correctly.









Program Flowchart

Introduction

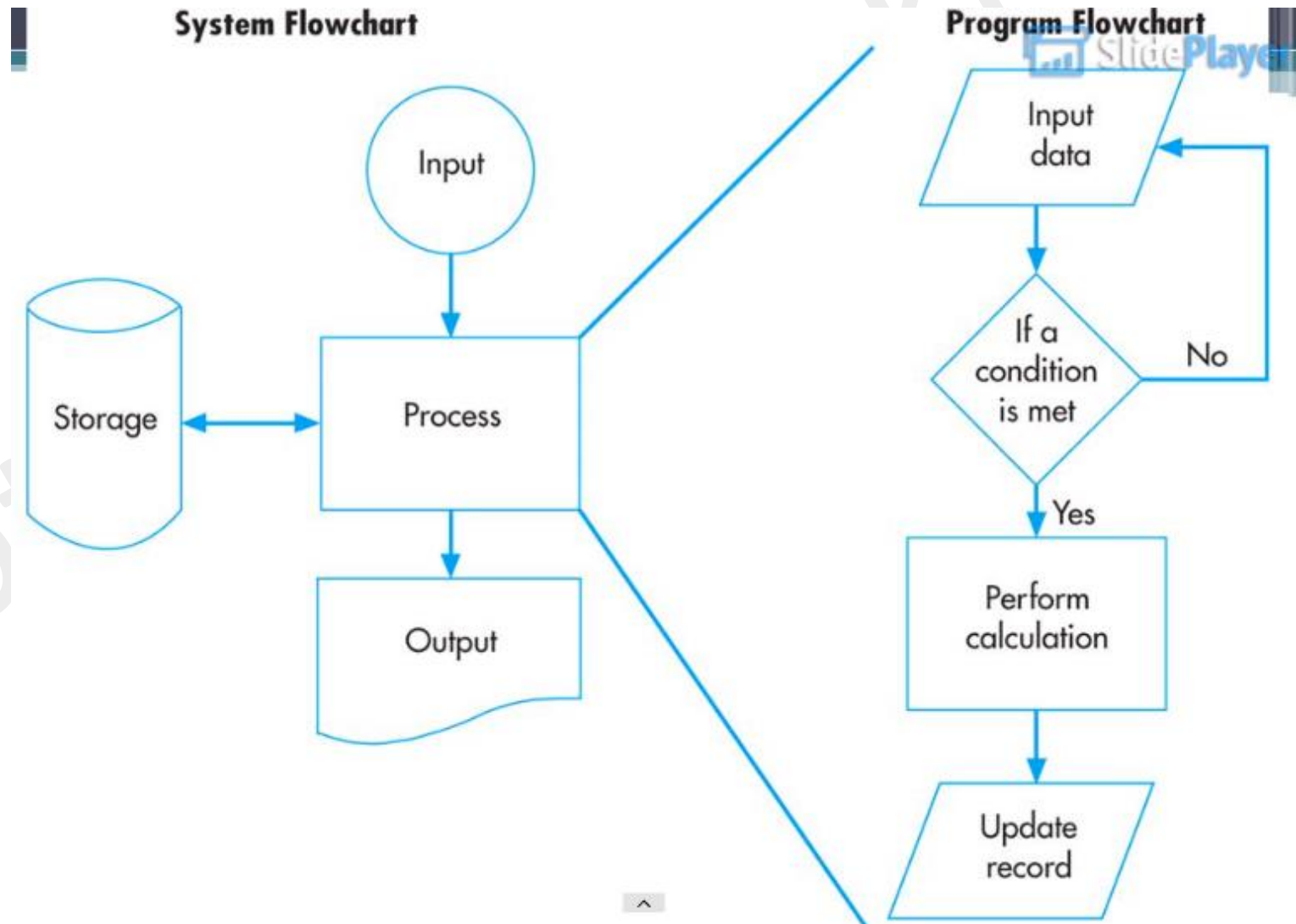
- Shows the controls placed internally to a program within the system.
- Illustrates the sequence of logical operations performed by a computer on executing a program.
- Follows an input-process-output pattern.
- Analyze the logic behind the program to process the code of the programming.

Subset of symbols

Name	Symbol	Use in flowchart
Oval		Denotes the beginning or end of a program.
Flow line		Denotes the direction of logic flow in a program.
Parallelogram		Denotes either an input operation (e.g., INPUT) or an output operation (e.g., PRINT).
Rectangle		Denotes a process to be carried out (e.g., an addition).
Diamond		Denotes a decision (or branch) to be made. The program should continue along one of two routes (e.g., IF/THEN/ELSE).
Circle		Connector. Connects two segment of a flow-chart when segments are on different pages

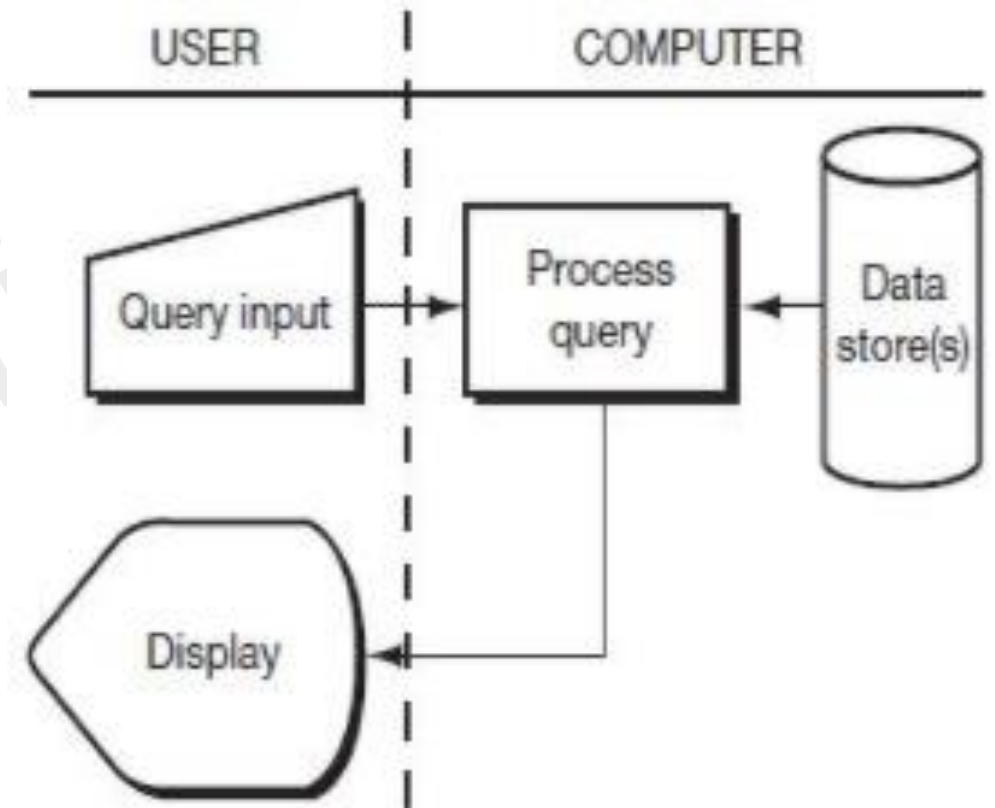
Introduction

- An entire information system is a collection of multiple programs. A program flowchart describes a single program. It is a good practice to draw a flowchart and identify how to solve the task using that program.
- The **main difference** between system flowchart and program flowchart is that a **system flowchart** represents an entire system while a **program flowchart** represents a single program.



Example

- A user gives a query leaf image request online into a computer. The computer process the query and matches with in one or more data stores and presents a response to the user.



System Flowchart

Example: Program flowchart (Process Query)

