INPUT CONTROLS

Input controls are critical for three reasons.

1) In many ISD the largest no. of controls exists in input subsystem, consequently auditors will often spend substantial time assessing the reliability of input controls
2) Input subsystem activities sometimes involve large amounts of routine, monotonous human intervention. Thus, they are error prone.
3) The input system is often the target of fraud. Many irregularities that have been discovered involve addition, deletion, or alteration of input transactions.

DATA INPUT METHODS

1) Recording medium a) Keyboarding b) direct reading (OCR, MICR, POS device, ATM)
2) Direct entry (PC, Touch screen, joystick, Voice, Video, Sound)

The following three aspects of input methods and how they are likely to affect auditors' assessment of control strengths and weaknesses:

1) As the amount of human intervention in the data input method increases, the likelihood of errors or irregularities occurring increases.
2) As the time internal between detecting the existence of an event and input of the event to an application system increases the likelihood of errors or irregularities occurring increases.
3) Use of certain types of input devices facilitates control within the input subsystem because they posses characteristics that mitigate against errors or irregularities.

Control advantages of using Point Of Sale (POS) terminal

1) Optical scanning of pre-remarked code improves pricing accuracy
2) Customers can verify accuracy and completeness of a sale because they can be provided with a detailed receipt
3) Improved control over tender because the terminal controls the cash drawer automatically dispenses change and stamps and handles any type of tender – cash checks, coupons.
4) Automatic check / credit card authorization. Customer can also enter PINs to authorize funds transfer from their account to vendor's account.
5) Maintenance of independent records of transactions undertaken through journal tapes
6) Netter inventory control through more timely information on item sales.

Control advantages of using Automatic Teller Machine (ATM)

1) Physical security over cash (antitheft features like alarms, camera, surveillance)
2) Maintenance of independent records of transactions undertaken via journal tapes and control counters
3) Cryptographic facilities to preserve the privacy of data entered
4) Software to guide customers through the input process, thereby minimizing errors.

SOURCE DOCUMENT DESIGN

Source documents are often used when there will be a delay between capture in the data about a state or event and input of that data into computer systems. From control point of view, a well designed source document achieves several purposes.

a. It reduces the likelihood of data recording errors
b. It increases the speed with which data can be recorded
c. It controls the work flow
d. It facilitates data entry into a computer system
e. It increases the speed and accuracy with which data can be read

Some important guidelines of effective source document design are:

i) Preprint all constant information
ii) Pre-numbered source documents
iii) Where possible provide MCQs

iv) Use tick marks to identify field size errors

v) Space items appropriately
vi) Provide titles, headings, notes and instructions
vii) Arrange fields for ease of use.
viii) Space items appropriately on forms

DATA ENTRY SCREEN DESIGN

If data is keyed into a system via a terminal, high quality screen design is important to minimizing input errors and to achieving an effective and efficient input subsystem.

1. Screen Organization

All the information needed to perform a task must be on a screen, yet users still should be able to identify quickly the information they require. Where screens must be used to capture a transaction the screens should be broken at some logical point. Symmetry can be achieved by grouping like elements together, balancing the number of elements on both sides of the screen, ensuring elements are aligned and using lank space and line delimiters strategically.

If the screen is used for direct entry input of data i.e. source document data entry the system must be an image of the source document in which the data is first captured and transcribed. In the former case the screen guides users though the data capture process. In the later case, users should be able to keep their eyes on the source document during the keying process and be required to view the screen only when they encounter some problem.

2. Caption Design

Captions indicate the nature of the data to he entered in a field on a screen. Design considerations include structure, size, type font, display, intensity, format, alignment, justification and spacing. Captions must be fully spelled out if a screen is used for direct data entry because the screen guides the user during the data capture process. If the data entry is made through source documents captions can be abbreviated because users can refer to the source document to obtain the full meaning of a caption.

Captions must be abbreviated clearly from their associated data entry field for e.g. upper case type font bight be used for all captions and lower case type font might be used for the data entered by the keyboard operator. Similarly different display intensities can be used.

3. Data Entry Field Design

Data entry field should immediately follow their associated caption. The size of a field should be indicated by using an underscore character. As each new character is entered into the field, the existing character is replaced.

Where direct data capture screens are used, completion aids used to reduce keying errors. For e.g. if a date must be entered the caption or the filed-size characters can be used to indicate date format:

DATE (YYMMDD):_____ DATE: YYMMDD

Radio boxes and check boxes (for small no. of options), list boxes (for large no. of options) and spin boxes are new frequently used for direct data entry capture.

4. Tabbing and Skipping

Automatic skipping to a new filed should be avoided in data-entry screen design for 2 reasons:

Firstly with an automatic skip feature, keyboard operators might make a field-size error that remains undetected because simply skips to the new field

Second, data-entry often are nor filled anyway

Thus, keyboard operators must tab to the next field.

5. Color

Colors can be used to aid in locating a particular caption or data item, to separate areas on the display, or to indicate a changed status (e.g. error situation). Color appears to reduce search time for an item on the screen and to motivate users better because the screen in more interesting.

6. **Response time** – is the interval that elapses between entry of a data item and the system's identification that it is ready to accept the new data item. As with all types of interactive tasks, the response time for data entry should be reasonably constant and sufficiently fast to sustain continuity in the task being performed.

7. **Display Rate –** is the rate at which characters or images on a screen are displayed. It is a function of the speed with which data can be communicated between the terminal and the computer. Data entry screens require a fast display rate. Users are unwilling to wait for long periods for captions and images to appear on a screen.

8. **Prompting and Help Facilities**

   Prompting facility provides immediate advice or information about actions users should take when they work with a data entry screen. A prompt often takes the form of a pop-up window containing an instructional message that appears automatically when a user moves the cursor to a particular field.

   A help facility provides look-up advice or information about actions users should take when they work with a data-entry screen. Help facilities are appropriate when ***(1)*** longer or more complex advices or information must be provided to users or ***(2)*** the advices or information will be needed infrequently.

DATA CODE CONTROLS - Data codes have 2 proposes. First, they uniquely identify an entity. Second, for identification purposes, codes are more compact than textual or narrative description because they carry fewer characters to carry given amount of information.

Data Coding Errors

i) **Addition** – extra character is added to the code
ii) **Truncation** – character is omitted from the code
iii) **Transcription** – wrong character is recorded e.g. 87942 coded as 81942
iv) **Transposition** – adjacent characters of the code are reversed e.g. 84942 coded as 78942
v) **Double transposition** – characters separated by one or more characters are reversed e.g. 87942 as 84972

Five factors affect the frequency with which theses coding errors are made:

i) **Length of the code** – longer codes are more error prone
ii) **Alphabetic numeric mix** –the error rate is lower if the alphabetics are grouped together and numerics are grouped together. Thus a code ASD123 is less error prone than A1S2D3.
iii) **Choice of characters –** if possible characters B, I, O, S, V, Z should be avoided because they are frequently confused with 8, 1, 0, 5, U, 2
iv) **Mixing uppercase/ lowercase fonts** – having to use shift key during keying breaks the keying rhythm

Types of coding systems

A coding system achieves following objectives:

i) **Flexibility –** easy to add new items or categories
ii) **Meaningfulness** – where possible a code should indicate the values of the attributes of entity
iii) **Compactness –** max. info is communicated in min. no. of characters
iv) **Convenience** – easy to encode, decode and key
v) **Evolvability –** a code can be adapted to changing user requirements

1. **Serial Codes -** assign consecutive numbers (or alphabetics) to an entity
2. **Block sequence codes –** assign blocks of numbers to particular categories of an entity. The primary attribute on which entities are to be categorized must be chosen, and blocks of numbers must be assigned for each value of attribute. For. E.g. if account no. are to be assigned to customers on the basis of discount allowed.

   101 Allen, 102 Smith } 3% discount allowed
   201 Elders, 202 Ball } 3.5% discount allowed

3. **Hierarchical Codes –** require selection of set of attributes of the entity to be coded and their ordering by importance. The value of the code is a combination of the codes for each attribute of the entity.

   C65 (division no.) 423 (dept. no.) 3956 (Type of expenditure)

4. **Association code** – the attributes of entity to be coded are selected, and unique codes are then assigned to each attribute value. Te codes can be numeric, alphabetic, or alphanumeric. The code for the entity is simply the concatenation of the different codes assigned to the attributes of the entity.

   SHM32DRCOT where SH = Shirt M = Male 32 = 32 cm, neck size
   DR = dress shirt COT = cotton fabric

CHECK DIGITS

Errors made in keying data can have serious consequences. For e.g. keying the wrong stock no. can result in a large quantity of wrong inventory being dispatched to a customer.

Check digit is a digit added to a code that enables the accuracy of other characters in the coded to be checked. The check digit can act as a prefix or suffix character or it can be placed somewhere in the middle of the code. When the code is entered, a program recalculates the check digit to determine whether the entered check digit and the calculated check digit are the same. If they are same, the code is most likely to be correct and vice versa.

Common systems are modulus 11 systems.

Example – check digit for 6312

i.	6	3	1	2	
ii.	5	4	3	2	(1 left foe check digit)
i x ii.	30	12	3	4	= 49 divide by 11 = 4 remainder 5
					---> 11 - 5 = 6

Therefore the code will be 6 3 1 2 6 . Now Check is digit by putting wrong code

6	3	2	1	6
5	4	3	2	1
30	12	6	2	6 = 56 divide by 11 = 5 remainder 1

Since it is not divisible by 11 the code is wrong.

BATCH CONTROLS

There are two types of batches: physical and logical batches

Physical batches – are groups of transactions that constitute a physical unit. I.e. source documents assembled into batches and tied together and then given to the data-entry clerk to be entered into an application system at a terminal.

Logical batches – are groups of transaction bound together on some logical basis. For e.g. different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions that they have entered. The input program logically groups transaction entered on the basis of the clerk's identification number. After some period has elapsed, it prepares controls totals for reconciliation with the clerk's controls totals.

Batch controls are based on total monetary amount, total items, total documents or hash totals. Batch totaling should be accompanied with adequate follow-up procedures, to ensure that all documents are included in batch, all batches are submitted for processing, all batch are accepted by the computer and controls exists over resubmission of rejected items.

Means of batch control

Two documents are needed to help exercise controls over physical batches:

i) ***Batch cover sheet*** **–** contains batch no., controls totals of batch, date, space for sign of personnel who have handled the batch.

ii) ***Batch control register*** **–** records the transit of physical batches b/w various locations within an org.

Three types of control totals can be calculated to identify errors

i) Financial totals ii) hash totals iii) Document/record counts

DATA VALIDATION AND EDITING

Procedures should be established to ensure that input data are validated and edited as close to the point of origination as possible. Preprogrammed input formats ensure that data are input to the correct field in the correct format.

Data validation identifies data errors, incomplete or missing data and inconsistencies related data items.

For data validation checks, consider 4 types that can be undertaken when input data that is keyed in at a terminal:

INPUT AUTHORIZATION (online or manual) – verifies that all transactions have been authorized and approved by management and to ensure that authorized data remains unchanged.

Types of authorizations include:

- Signature on batch forms
- Online access controls to ensure only authorized individuals may access data
- Unique passwords
- Terminal or client WS identification limits input to specific terminals or WS and to individuals.

- A well designed source document may increase the speed and accuracy with which data can be recorded, controls workflow, increases the speed and accuracy.

TYPES OF DATA INPUT VALIDATION CHECKS

1. Field checks

i) **Missing data / blanks** – does the field contain blanks where the data must be present?
ii) **Alphabetics / numerics**
iii) **Range check** – data should be within the predetermined range of values i.e. codes ranging from 100–250.
iv) **Check digit** – is the check digit is valid for the value in the field.
v) **Size –** if the variable length fields are used and permissible size is defined, the input should adhere to that.
vi) **Sequence check** – control no. follows sequence and any out of sequence or duplicated control nos. are rejected.
vii) **Limit check** – data should not exceed the predetermined amount i.e Rs. 1,000
viii) **Validity check** – checking data validity in accordance with predetermine criteria (yes / no.)
ix) **Table look-ups** – input data complies with predetermined criteria maintained in a computerized table of possible values i.e. city code.
x) **Format mask** – data entered into a field might have to confirm to a particular format (yymmdd)
xi) **Master reference** – if the master file can be referenced at input, is here a master file match for the key filed.

2. Record checks

i) **Logical relationship check** – the hire data of an employee required to be more than 16 yrs past of his/her date of birth.
ii) **Reasonableness check** – input data is matched with predetermined reasonable limits i.e. orders for no more than 20 watches
iii) **Sequence check –** the input program might check the sequence of physical records it receives.
iv) **Valid sign numerics –** the contents of one field might determine which sign is valid for numeric field. For e.g. if a transaction type field indicates cash payment has been received from a customer, the amount field should have, say, a positive sign.

3. Batch checks

i) **Control totals**
ii) **Transaction type –** all input records in a batch might have to be a particular type.
iii) **Batch serial number –** all input records in a batch might have to include a sr. no. that has been assigned to the batch
iv) **Sequence check –** the input records in a batch might have to follow a particular order.
v) **Duplicate check**

ERROR REPORTING AND HANDLING – controls to verify that data are accepted into the system correctly and that input errors are recognized and corrected. Corrections to data should be processed through normal data conversion process and should be verified, authorized and reentered to the system as a part of normal processing.

Input error handling can be processed by:

i) Rejecting only transactions with errors
ii) Rejecting the whole batch of transactions
iii) Accepting batch in suspense
iv) Accepting batch and flagging error transactions

INSTRUCTION INPUT

Ensuring the quality of instruction input to an application system is a more difficult objective to achieve. During instruction input, however, users, often attempt to communicate complex actions that they want the system to undertake. Following are the application system used to communicate instruction to an application system.

1. Menu driven languages

Menu is the simplest way to provide instruction to an application system. The system presents users with a list of options. Users then choose an option. The following guidelines should reduce the no. of errors that are likely to occur using menu input:

i) Menu items should be grouped logically so they are meaningful and memorable

ii) Menu items should follow any natural order, ordered by frequency of occurrence and long menus by alphabetical order.

iii) Menu should be fully spelled, clear, concise

iv) The basis for selecting a menu item should be clear for e.g. numbers, a mnemonic abbreviation

v) Where other output is displayed on the screen, the menu should be clearly differentiated.

2. Question answer dialogue

Used primarily to obtain data input. For finding of NPV system asks questions like discount rate, initial investment, no. of periods, cash flow per period etc. and the user responds. A well designed question-answer dialog makes clear the set of answers that are valid. In those cases in which the required facility answers are not obvious, a help facility can be used to assist inexperienced users.

3. Command languages – require users to specify commands to invoke some process and a set of arguments that specify precisely how the process should be executed For e.g., SQL is a database interrogation language that uses a command-language format.

- ☞ To facilitate recall of commands, command names should be meaningful.
- ☞ To reduce typing effort, it should be possible to truncate (shorten, abbreviate) commands

4. Forms based languages - Forms-based languages can be successful if users solve problems in the context of input and output forms. In these cases syntax of the language corresponds to the ways users think about the problem. As a result, input errors are reduces, and the language tends to be used effectively and efficiently.

5. Natural languages – are the subject of substantial research and development efforts. Its goal is to enable relatively free form natural language interaction to occur b/w users and users and an application system, perhaps via speech production/recognition device. Current natural languages have following limitations.

i) They donot always cope with the ambiguity and redundancy present in natural language for e.g., the meaning

ii) Substantial effort sometimes must be expanded to establish the lexicon (glossary, word list) for the natural language interface. Users must define all possible works they could use

iii) Even minor deviations outside the lexicon established for the application domain can cause problems.

iv) Users still need some training when they employ natural language interfaces.

6. Direct manipulation languages

Some user interface application systems employ direct manipulation to enter commands and data i.e. spreadsheet. There are 3 attributes are identifies of a direct manipulation interface ***(1)*** visibility of the object of interest ***(2)*** rapid, reversible, incremental actions and, ***(3)*** use of direct manipulation devices e.g. mouse. Examples are:

i) Electronic spreadsheet – users see visual image on the spreadsheet and its associated cell values. They can alter values by using a mouse to move the cursor to the cell to be altered and keying of new value.

ii) Electronic desktops – users see an image of a desktop with an in-basket, an out-basket, a thrash basket, a set of files and so on. They can manipulate these objects using a mouse. For e.g. files to be deleted can be moved to the trash basket.

It often provides a more error free, effective and efficient interface that traditional menu or command-oriented interfaces.

AUDIT TRAIL CONTROLS

Accounting audit trails - They must records the origin of, contents of and timing of the transaction. The audit trail might record the following:

i) The identify of the originator of the instruction
ii) The time and date when the instruction was entered
iii) The identifier of the physical device used to enter the data into the system.
iv) The type of instruction entered and its arguments
v) The results produced in light of the instructions

Operations audit trails – is an important means of improving effectiveness and efficiency of the sub-system. The audit trail might record the following:

i) Time to key in a source documents
ii) No. of read errors made by and Optical scanning device
iii) No. of keying errors identified during verification
iv) Frequency with which an instruction in a command language is used, and
v) Time taken to invoke an instruction using a light pen versus a mouse

EXISTENCE CONTROLS

Existence controls that relate to data in input subsystem is critical. In an application system's master files are destroyed or corrupted, recovery could involve going back to a previous version of the master files and reprocessing input against these files. Recovery cannot be possible if backup copies are maintained at offsite location.

If the input files are also destroyed then recovery has to be made from source documents or hardcopy transaction listings. Thus, source documents or transaction listings should be stored securely until they are no longer needed for backup purposes.

COMMUNICATION CONTROLS

Communications infrastructure is a collection of devices and procedures for communicating signals in the form of a message between a sender and receiver.

Transmission components (means of transmission and the data encoding or channeling techniques i.e. multiplexing) or switching components (data transmission and reception devices and user circuits and packet switching) are used to reach the final destination.

COMMUNICATION SUBSYSTEM EXPOSURES

A) Transmission impairments – can cause differences between data send and received

B) Data can be lost or corrupted through **component failure**

C) Subversive threats – hostile party could seek to subvert data that is transmitted though the subsystem

A) TRANSMISSION IMPAIRMENTS

Reasons For Degradation Of Signal During Transmission

1. **Attenuation –** as the signal transmits to a long distance along a transmission medium, its amplitude decreases. This is especially apparent when the medium is copper wire. In case of analog signals amplifiers are used after a signal traveled a certain distance to boost the signal to higher amplitude (strength). In case of digital signals repeaters are used.
2. **Delay distortion** – occurs when the signal is transmitted through bounded media (twisted pair). Different frequencies pass through bounded media with different velocities. Thus, signals are distorted because their different frequency components are subject to different delays. Consequently the signal is arrived at receiver with varying frequency and can result in misinterpretation of data.
3. **Noise –** is the random electric signal that degrade performance in the transmission media. If the current is already in wire, this will distort message.

B) COMPONENT FAILURE

1. **Transmission Media**
2. **Hardware** (ports, modems, amplifiers, repeaters, multiplexers, switches, concentrators)
3. **Software** (packet switching software, polling software, data compression software)

Hardware and software failure can occur for many reasons – for e.g. failure in integrated circuit, disk crash, a power surge, insufficient temporary storage or program bugs.

C) SUBVERSIVE THREATS – can be active or passive

In a passive attack the intruder's attempt:

- to learn the characteristics the data being transmitted, so privacy of data is violated
- read and analyze the clear text source and destination identifiers attached to a message for routing purposes, and the content of data remains same
- examine the length an frequency of message

Examples are traffic analysis, Release of message content, invasive tap

In an active attack, intruders could

- ***insert*** a message in the message stream being transmitted
- ***delete*** the message being transmitted
- ***modify*** the contents of message
- ***duplicate*** messages
- ***alter*** the order of message
- ***deny*** message services b/w sender and receiver by corrupting, discarding or delaying messages

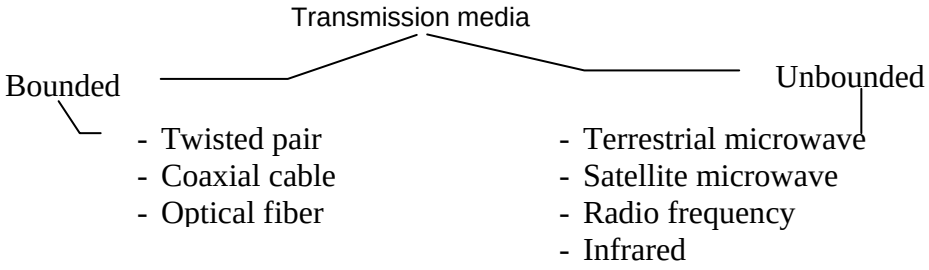
PHYSICAL COMPONENT CONTROLS

To reduce expected losses in the communications subsystem is to choose physical components that have characteristics that make them reliable

The following subsections give an overview of how physical components can affect communication subsystem reliability.

A. TRANSMISSION MEDIA

It is a physical path along with a signal can be transported between the sender and receiver. Various types of transmission media can be used



a) Copper Wire (Twisted Pair) – circuits are two insulated wires twisted around each other. One wire carries electricity to the telephone or modem and the other carries electricity away from the telephone or modem. It allows only low rate of data transmission. Amplifiers for analog signals and repeaters for digital signals mist be place every few Km if data is to be transmitted over long distances. Highly susceptible to crosstalk and noise.

b) Coaxial cables – have higher capacity than twisted pairs. A single coaxial cable can carry voice, data and video signal at one time. Moderate level of data transmission. Amplifiers or repeaters must be installed for long transmission of data.

c) Fiber optic cable – which use hair thin glass fibers to carry binary signal as flashed of light. Fiber optic systems have low transmission loss as compared to twisted pairs; the speed of operation is that of light.

d) Terrestrial microwave – permits moderate rate of data transmission over relatively long distances. Line of sight transmission is required, thus a microware station is required every 40 Km. Microware transmission is highly susceptible to various forms of interference.

e) Satellite microware – permits moderate rate of data transmission over long distances. Line of sight transmission is maintained by having the satellite orbit the earth so it remains stationary with respect to its earth stations. It is also highly susceptible to interference and can be wire tapped easily.

f) Radio frequency – permits moderate rate of data transmission over moderate distances. Radio frequency is also omni directional. It is also highly susceptible to interference and can be wire tapped easily.

g) Infrared – permits moderate rates of data transmission over short distances. It is also highly susceptible to interference and can be wire tapped easily.

B. COMMUNICATION LINES

The reliability of data transmission can be improved by choosing a private communication line. Private lines are dedicated to service a particular user. They have 2 advantages:

They allow higher rates of data transmission

Second they can be conditioned, i.e. the carrier ensure the line has certain quality attributes. A conditioned line limits the amounts of attenuation, distortion and noise that its users will encounter.

C. MODEMS

They are the data communication equipment devices that provide connections for computers over telecommunication network.

Modems convert computer digital signals into analog signals that can be transmitted over telecommunication lines and vice versa. They undertake three functions that affect the reliability of the communication subsystem.

- First, they increase the speed with which the data can be transmitted over communication line by using multiplexing technique.
- Second, modems can reduce the no. of line errors that arise through distortion using a process called equalization. It continually measures the characteristics of a line and performs automatic adjustments for attenuation and distortion.
- Third, modems can reduce the no. of line errors that arise through noise.

D. PORT-PROTECTION DEVICES – are used to mitigate exposures associated with dial-up access to computer system. When users place a call to the system a connection is established with port-protection device and following functions are performed.

i) Dial back security

ii) Users could be required to provide passwords before the port-protection device will allow them access to the host system.

iii) Port protection devices could maintain an audit trail of all successful and unsuccessful accesses to host system.

E. MULTIPLEXERS AND CONCENTRATORS

They allow the bandwidth to be used more efficiently. The common objective is to share the use of a high cost transmission line among many messages that arrive at the multiplexor or concentration point

Multiplexers allows a physical circuit to carry more than one signal at one time when the circuit has more bandwidth than required by individual signals. It can also link several low speed lines to enhance transmission capabilities.

Concentrators use schemes whereby some number of input channels dramatically shares smaller number of output channels on a demand basis. Three common types of concentration techniques are message switching, packet switching and line switching.

In *Message switching,* a complete message is sent to the concentration point and stored until a communication path can be established.

In *packet switching,* a message is broken into small fixed length packets, the packets are routed individually through the network depending the availability of channel of each packet.

In *line switching,* a device establishes temporary connection between input and output channels where the no. of input channels exceeds the number of output channels.

i) Both allow more efficient user to be made of available channel capacity

ii) Concentration techniques can route a message over a different path if particular channel fails

iii) These functions are often incorporated into an intelligent front-end processor that performs other function such as message validation and protocol conversion

iv) Both channels help to protect data against subversive attacks. Wiretappers have great difficulty over a channel connected to multiplexor or concentrator

F. LINE ERROR CONTROLS

Error detection

Line errors can be detected by either using loop (echo) check or building some form of redundancy check.

Loop check involves the receiver of the message sending back the message received to the sender. The sender checks the correctness of the message received by the receiver buy comparing it with a stored copy of the message sent

Redundancy involves attaching extra data to a message that will allow corrupted data to be detected. Two forms of redundancy based error detection methods are:

Parity checking **–** the transmitter adds an additional bit to each character prior to transmission. The parity bit used is a function of the bits making up the character. The recipient performs the same function on the received data and compares it to the parity bit.

Cyclic Redundancy Check – the block of data to be transmitted is treated as a binary no. This no. is then divided by a prime binary no. The remainder is attached to the block to be transmitted. The receiver recalculates the remainder to check whether any data in the block has been corrupted.

Error correction

When line errors have been detected, they must be corrected using following 2 methods:

Forward error correcting codes enable line errors to be corrected at the receiving station

Retransmission of data in error (backward error correction), the sender sends the data again if the receiver indicated the data has been received in error.

FLOW CONTROLS

Flow controls are needed because 2 nodes in a network can differ in terms of the rate at which they can send, receive ad process data. We use following methods:

Stop and wait flow control – using this approach the sender transmits a frame of data. When the receiver is read to accept another frame, it transmits acknowledgement to the sender. On receipt of acknowledgement the sender transmits another frame.

In *sliding window flow controls* approach both the sender and receiver have buffers.

TOPOLOGICAL CONTROLS

A) LOCAL AREA NETWORK

LAN have three characteristics

i) They are privately owned networks
ii) Provide high speed communication among nodes
iii) They are confined to limited geographical areas

1) Bus topology – nodes in the network are connected in parallel to a single communication line. A *passive tap is used* to transmit and receive data from the bus. Data is transmitted along both directions of the bus. Following are the auditor's controls perspectives.

i) A bus degrades performance of transmission medium because the taps that connect to each node introduce attenuation and distortion because of higher data traffic.
ii) Because taps are passive, the network will not fail if the node fails
iii) Because all nodes have access to traffic on the network, messages not intended for a particular node can be accessed either deliberately or accidentally. Thus controls must be implemented i.e. encryption

2) Tree topology – nodes in the network are connected to a branching communication line that has *no closed loops*. As with a bus, each node *uses a passive tap* to broadcast data onto and receive data from the communication line. Auditors have same control perspectives as on bus topology.

3) Ring topology – nodes in the network are connected through *repeaters (active device)* to a communication line that is configured as a *closed loop.* Repeater inserts, receives and removes data from the line. Normally unidirectional rings are used; however, bi-directional rings can be used to accommodate failures. Following are the auditor's controls perspectives:

i) Repeaters donot add attenuation and distortion and transmit a clean signal
ii) Because repeaters are active components, therefore, they will bring down the network if they fails. To compensate it repeaters have by pass mode.
iii) Because all traffic routed through each node's repeater, messages not intended for a particular node can be accessed either deliberately or accidentally. Thus controls must be implemented i.e. encryption

4) Star topology – nodes in the network are connected in a point-to –point configuration to a central hub. The central hub can act as a switch. Following are the auditor's controls perspectives:

i) The reliability of the central hub is critical. If the central hub fails, entire network will down
ii) Servicing and maintenance is very easy. Problem can be diagnosed from central hub and faults can be located quickly.

5) Hybrid topology – various types of hybrid topologies are used in LAN. For e.g. in the star-bus topology, nodes are connected via relatively long communication lines to a short bus.

B) WIDE AREA NETWORK – have following characteristics:

i) They often encompass components that are owned by other parties (e.g. telephone co.)
ii) They provide relatively low speed communication among nodes
iii) They span large geographical area

With the exception of bus topology that is used to implement LAS can also be used to implement WAN. The most commonly used topology is mesh topology. In mesh topology every node often must communicate with every other node. A path b/w nodes is established using any of the concentration techniques previously discussed: message switching, packet switching, line switching

From controls point of view mesh topology is inherently reliable because data can be routed via alternative paths through the network.

CHANNEL ACCESS CONTROLS

Polling / non contention methods
Contention methods

CONTROLS OVER SUBVERSIVE THREATS

1. **Link encryption –** The sending node encrypts the data it receives and then transmits the data in encrypted form to the receiving node. The receiving node subsequently decrypts the data, reads the destination address from the data, determines the next channel over which to transmit the data and encrypts the data under the key that applies to the channel over which the data will next to be sent. It reduces expected losses from traffic analysis, as the message and its associated source and destination identifiers can be encrypted. Thus, the wiretapper has difficulty determining the identity of sender and receiver.

   If an intermediate node in the network is subverted, all traffic passing through the node will be exposed.

2. **End-to-End encryption –** can be used to protect the integrity of data passing b/w sender and receiver. Thus, cryptographic features must be available to each sender and receiver and the encrypted data is not decrypted until it reaches the receiver. It provides only limited protection against traffic analysis.

3. **Message authentication code (MAC)**

   In EFT, a control used to identify changes to a message in transit is a MAC. MAC is calculated by applying an algorithm and a secret key to selected message. The MAC is then appended to the message and sent to he receiver, who recalculated the MAC on the basis of message received to determine whether the calculated MAC and the received MAC are equal.

4. **Message authentication code (MAC) –** used to detect an attack on the order of messages that are transmitted. If each message contains a sequence no. and the order of sequence no. is checked. These attacks will not be successful. Further more; to prevent message duplication, seq. no. must be used b/w sender and receiver. A unique identification no. must be established for each communication session; within this identification no. each message seq. no. must be unique.

5. **Request response mechanism –** used to identify attacks by an intruder aimed at denying message services to a sender and receiver. In this mechanism a timer is placed with the sender and receiver. The timer periodically triggers a control message from the sender. Because the timer at the receiver s synchronized with the sender, the receiver must respond to show that the communication link not been broken.

INTERNETWORKING CONTROLS

It is the process of connecting two or more communication networks together to allow the users of one network to communicate with the users of other network. The overall set of interconnected networks is called an *Internet*. An individual network within Internet is called a *sub-network.* Three types of devices used to connect sub networks to internet.

1. **Bridges –** devices that connect 2 similar LAN (e.g. one token ring network to another)

2. **Gateways** – Perform protocol conversion to allow different types of communication architectures to communicate with one another

3. **Routers –** switching devices, by examining the IP address, can make intelligent decision to direct the packet to its destination.

Bridges, routers and gateways perform several useful control functions. First, because they allow the total network to broken up into several smaller networks, thereby improve the overall reliability of the network (failure in one node donot effect others). Second, allow user to keep different types of applications to different sub-networks (High exposure EFT massages routed over high security sub-network and vice versa). Third, they restrict access to sub-networks only to authorized personnel.

DATABASE CONTROLS

The primary type of data maintained in the database subsystem has been

Declarative data – data that describes the static aspects of real-world objects and associations among theses objects i.e. a payroll file store info about the pay rates for each employee, the various positions among organization and the employees who have assigned to each position.

Procedural data – data that describes the dynamic aspects of real-world objects and the associations among theses objects i.e. set of rules how a portfolio manager makes decisions about which stocks and bonds to choose for investment purposes.

When both declarative and procedural data is combines, the databases is called **knowledge base**

With the emergence of huge databases and increasing use of DSS and EIS, there has been renewed interest in how data bases should be structured to allow recognition of patterns among data, thereby facilitating knowledge discovery of decision makers.

Huge databases that contain integrated data, detailed and summarized data, historical data and metadata are sometimes called *data warehouse.* Databases that contain a selection of data from a data warehouse that is intended for a single function are called *data marts.* The process of recognizing patterns among data in data warehouses or data marts is sometimes called *data mining.*

ACCESS CONTROLS – prevent unauthorized access to and use of data.

A) DISCRETIONARY ACCESS CONTROLS

In a RDBMS, user may be authorized to do the following:

i) Create a schema (plan, scheme)
ii) Create, modify or delete views associated with the schema
iii) Create, modify or delete relations associated with the schema
iv) Create, modify or delete tuples in relations associated with the schema

These access privileges are given to users who are designated as owners of a particular schema. Some important types of restrictions are as follows:

1. **Name dependent restrictions/content independent restrictions**– users have access to a named data resource i.e. payroll clerk can read only the name of persons, their locations, and their salary.
2. **Content dependent restrictions** – access have been permitted or denied depending on its contents. For e.g. personnel clerk is not permitted to access an employee if it exceeds Rs.100,000
3. **Context dependent restrictions** – access have been permitted or denied depending on the context in which they are seeking access. Personnel clerks are not permitted access to the names of employees whose salary exceeds Rs.100,000 unless they are seeking to execute some type of statistical function on salary data.
4. **History dependent restrictions**

If the owner grants privileges to another user, the privileges might need to be exercised over the extent to which propagation that occurs. Different types of controls might need to be exercised over the extent of propagation that occurs. One type is a ***horizontal propagation control***, which limits the no. of users to whom a user can assign privileges. Another type is ***vertical propagation controls*** which limit the depth of propagation or no. of users in a sequence can be granted privileges.

B) MANDATORY ACCESS CONTROLS

Under this approach users are assigned clearance level and resources are assigned classification level. User access is governed by security policy. Users are not allowed to read a resource unless their clearance level is greater that or equal to the resource's classification level.

APPLICATION SOFTWARE CONTROLS

A) UPDATE PROTOCOLS – seeks to ensure that changes to data bases reflect changes to the real-world entities and association between entities that data in the database is supported to represent. Some of the more important protocols are as follows:

1. **Sequence check transaction and master files –** In the batch run, the transaction file is often sorted prior to the update of the master file or the table in the database. In some cases, aster file or table to be updated might also be sorted in a particular order.

2. **Ensure all records on files are processed –** If a master file is maintain in sequential order, correct end-of-file protocols must be followed in an update program to ensure records are not lost from either master file or transaction file.
3. **Process multiple transactions for a single record in the correct order** – for e.g. sales order plus a change of address might have to be processed against a customer master record. The order in which the transactions are processed can be important i.e. firstly, address to be updated and then the sales order, a customer might be billed at previous address. Different types of transactions must be given transaction codes so they can be sorted in particular order before being process in master file.
4. **Maintain a suspense account –** The suspense account is the repository for monetary transactions for which a matching master record cannot be found at the time an update is attempted. Mismatch can occur due to wrong entry of account no. or the transaction might arrive before the master record is created.

B) REPORT PROTOCOLS – has been designed to provide info to users of database that will enable them to identify errors or irregularities. We examine three such protocols

1. **Print control data for internal tables (stranding data)** – many programs have internal tables they use to perform various functions for e.g. pay rates table is used to calculate gross pays, table of prices for invoices etc. Even changes are made to standing data, internal table might still be printed periodically to check for any unauthorized changes or the corruption of data. If the table is too large some type of control total can be taken and check it from previous control total.
2. **Print run-to-run control totals -** verify data values through the stages of application processing.
3. **Print suspense account entries –** to ensure that all suspense account transactions are cleared suspense account report must be prepared. It should remind users that they must take action to clear the errors if they are not removed form the error file promptly.

CONCURRENCY CONTROLS

Data integrity can be violated when two processes are allowed concurrent access to a data item. One process could read and update a data item at the same time as another process reads and updates the data item. The effect of one update operation can be lost. Locking out one process while the other process completes its update can lead to a situation called deadlock in which two processes are waiting for each other to release a data item that the other needs.

A widely accepted solution to deadlock is two phases locking, in which all the data items needed to propagate the effects of a transaction are first obtained and locked from other processes. The data items are not released until all updates on the data items have been completed.

CRYPTOGRAPHIC CONTROLS – can be used to protect the integrity of data in the database. In case of portable storage media, encryption can be carried out by a cryptographic device in the controller. The privacy of data is stored if the device is stolen, but one user's data is not protected from another user. For this cryptographic keys must be assigned to the owner of the data and those users allowed accessing the data.

FILE HANDLING CONTROLS – are used to prevent accidental destruction of data contained on a storage medium by an operator, user or program. They include internal labels, generation numbers, retention dates, control totals, magnetic tape file protection rings, read-only switches and external labels.

AUDIT TRAIL CONTROLS

Accounting Audit Trail

First it must attach a ***unique time stamp*** to all transactions. It confirms a transaction has ultimately been reached the database and identifies a transaction's unique position in the time series of events that occurred to a data item.

Second, database subsystem must attach ***beforeimages and afterimages*** of the data item. If the transaction modifies an existing data item value, the value of the data item before it is updated and after it is updated must be stored in transaction audit trail entry. 1) They facilitate inquiries on the audit trail because the effects of the transaction on the database can be determined immediately 2) redundancy for time stamp because fraudulent deletion of an audit trail entry or alteration of time series can be detected vi a mismatch b/w the after image of a transaction and before image of subsequent transaction.

Operational audit trail

In operations audit trail, auditor is concerned about ***response time*** and ***resources consumed.***

EXISTENCE CONTROLS

The whole portion of data base can be lost through 5 types of failures:

TYPES OF DATABASE FAILURES

1. **Application program error** – can update data incorrectly because it contains a bug
2. **System software error** – may be in OS, DBMS, network management system or a utility program. The error may lead erroneous update or corruption of data held by the database.
3. **Hardware failure –** data may be lost due to hardware failure or malfunctioning.
4. **Procedural error** – can be made by operator that can damage the database.
5. **Environmental error** – such as flood, sabotage etc.

The existence controls includes establishing and implement data back-up and recovery procedures to ensure database availability. Various forms of backup recovery are:

BACKUP STRATEGIES

1. **Grandfather, father, son strategy –** involves maintaining two historical backups i.e. if the current version (son) of master file is corrupted it can be recovered from its previous version (father) and the log of transaction update it to the new version. If the previous version of master file is damaged during recovery process, the next older version is updated with the log of transaction. In this strategy the input master file must be kept physically intact and the transaction file used to effect updates also must be kept.

2. **Dual recoding / Mirroring –** involves maintaining 2 separate copies of the same database at different physical locations. Advantage is that it permits the database to be available continuously e.g. types of online reservation systems. It is costly to maintain. It is also known as replication.

3. **Dumping –** it involves copying of the whole or critical part of the database to a medium from which it can be rewritten. Both physical and logical dumps can be created. *Physical dumping* involves reading and copying the database in the serial order of the physical records on the storage medium. *Logical dumping* involves reading and copying the database in the serial order of the logical records in a file.

4. **Logging –** involves recording a transaction that changes the database or an image of the record changed or an image of a record changed by an update action. It includes recording all the events that update, create or delete any record in the database. Three types of logs can be kept:
   i. Transaction logs to allow reprocessing of transactions during recovery.
   ii. Beforeimage logs to allow rollback of the database – each time record is update its image before the update us logged. If a transaction fails before it commits all its changes to the database, the database can be rolled back to the last commit point
   iii. Afterimage logs to allow roll-forward of the database – after a record has been updated by the transaction its image in copied onto the log. If for e.g. the disk then fails, recovery is accomplished by rolling forward using the latest dump of the database and replacing the dump version of the record with afterimage version from the log.

5. **Residual dumping –** periodic full dump of database. Involves high cost, takes substantial time and dumps waste resources.

6. **Differential file / Shadow paging backup and recovery strategy –** involves keeping the database intact and writing changes to the database to a separate file. In due course these changes are written to the database. If failure occurs before the changes are applied the intact database constitutes a prior dump of the database. Providing a log of transactions has been kept, these transactions can then be reprocessed against the database.

CONTROL PROCEDURES

1. Establish definition standards and closely monitor for compliance
2. Establish and implement data back-up and recovery procedures to ensure database availability.
3. Establish various levels of access controls for data items, tables and files to prevent inadvertent or unauthorized access.
4. Establish controls to ensure only authorized personnel can update the database.
5. Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database.
6. Perform database reorganization to reduce unused disk space and verify defined data relationships
7. Use database performance monitoring tools to monitor and maintain database efficiency.

OUTPUT CONTROLS

BATCH OUTPUT PRODUCTION AND DISTRIBUTION CONTROLS

Batch output is output that is produced at some operations facility and subsequently distributed to or collected by the custodians or users of the output. Production and distribution controls over batch are established to ensure that accurate, complete and timely output is provided only to authorize custodians.

Stages in production and distribution of batch output

1. Storage of stationery supplies
2. Report program execution
3. Queuing / spooling
4. Printing
5. Output collection
6. User / client services review
7. Output distribution
8. User review
9. Output storage
10. Output retention
11. Output destruction

1. Stationery supplies storage controls

Whenever preprinted stationary us used, auditors should check to determine whether the organization exercises careful controls over the stationery.

- Stationery suppliers should produce preprinted stationery only under proper authorization and provide preprinted stationery only to authorized persons.
- Store preprinted stationery securely
- Control access to preprinted stationery i.e. only to authorized personnel
- Pre-number preprinted stationery
- Store signature stamps and preprinted stationery for negotiable instruments at separate physical locations

2. Report program execution controls

- First, authorized persons should be able to execute them i.e. a bank would want to restrict the execution of the program that prints PINs to only a few trusted employees.
- Second, the action privileges assigned to authorized users should be appropriate to their needs for e.g. to limit the no. of copies of a report, or to limit production of the report to certain times of the day
- Third, report programs that produce a large amount of output should include checkpoint / restart facilities. It can reduce the amount of work that has to be redone when some type of system failure occurs

3. Queuing / spooling /printer fine controls

If a program cannot write immediately to a printer, the output is queued or spooled. This spooling leads to two control problems. First, printer files provide opportunities for unauthorized modifications to and copying of reports. Second, spooling software might allow operators to return to some prior intermediate point and to restart printing of a report. Unauthorized copies can be produce in this way.

Auditors must evaluate:

- Contents of printer files cannot be altered
- Unauthorized copies of printer files cannot be made
- Pinter files are printed only once
- If copies of printer files are kept for backup and recovery, they are not user to make unauthorized copy

4. Printing controls – have three purposes

i) To ensure that reports are printed on the correct printer;
ii) To prevent unauthorized parties from scanning sensitive data that are printed on reports;
iii) To ensure that proper control is exercised over printing negotiable forms or instruments.

Controls

i) users might be permitted to activate printing of sensitive reports from workstations that can access only secure printers
ii) users might be trained to checked that they have selected the correct printer.
iii) When impact printers are used, no printer ribbons are used in the impact PIN mailers
iv) If preprinted stationary is used, the no. of forms generated should, be reconciled against the no. of forms received from stationery supplies.

5. Output / report collection controls

When output has been produced, it should be secured to prevent loss or unauthorized removal. They should collect the output promptly and store it securely.

If user/client services group representatives have responsibility for collecting output, they should maintain records of the output they handle. For e.g. they should note the data and time when each output item was collected and the state of the output received and the identity of the group representative

Controls should exist to identify when output is not collected promptly and secured.

6. User / client services review controls

Before output is distribute to users a user/client services representative might check if for obvious errors. Following types of checks could be undertaken:

i) Whether printed report is legible
ii) Whether quality of film output is satisfactory
iii) Whether tape cartridges or CD-ROM have been labeled properly
iv) Whether printed report are missing

These controls are exercise to deliver high quality products and incase of any irregularity responsibility can be fixed

7. Output / report distribution controls – distribution can occur in various ways:

i) Output might be place in locked bins that users clear periodically
ii) Output might be delivered directly to users
iii) Output might be mailed to users through e-mail or courier
iv) Output might be handover to users or user representatives

To exercise control over output distribution activities, records should be kept of the date and time at which output was distributed and the identity of the person who received the output. Logging of distribution report.

Where users or third parties are unknown to the user/client services group, they should be asked to identify and authenticate themselves.

Verification of receipt of reports – to provide assurance that sensitive reports are distributed properly, the recipient should sign a log as an evidence receipt of output

8. User review controls – user should perform reviews to detect errors and irregularities in output.

They might perform test calculations to check the accuracy or controls totals shown in output report, or they might undertake a physical count of some inventory items to check whether the amounts on hand correspond to those shown in an inventory listings.

9. Storage controls

i) First, output should be stored in an environment that allows it to be preserved for the period it is required. In this regard, various output media have different requirements in terms of the environments in which they should be kept.
ii) Second output must be stored securely
iii) Third, appropriate inventory controls must be kept over stored output.

10. Retention controls

A decision must be made on how long each type of output will be retained. This decision can affect the choice of output medium and the way in which the output is stored. The output must then be kept until retention date expires. Factors that affect retention date are: the need for archival reference of the report, backup and recovery needs, taxation legislation specifying a minimum retention time for data, and privacy legislation specifying a maximum retention time for data.

11. Destruction controls

When output is no longer needed or retention date expired, it should be destroyed.

BATCH REPORT DESIGN CONTROLS

i) Control information
ii) Report name
iii) Time and date of production
iv) Distribution list (including number of copies)
v) Processing period covered
vi) Program (including version number producing the report) – permits identification of originating system/program.
vii) Contact persons
viii) Security classification – alerts operators and user/client services representatives to the sensitivity of data contained in report.
ix) Retention date
x) Method of destruction – any special procedures needed
xi) Page heading
xii) Page number

ONLINE OUTPUT PRODUCTION AND DISTRIBUTION CONTROLS

1. Source Controls –

a) Where the output is computer generated the control objectives are:
   i) authorized, accurate, complete and timely transactions are generated and
   ii) These transactions are generated and transmitted only once.

   To achieve these objectives appropriate access and input controls should be in place.

b) Where the user invokes a program to access database and prepares output, the control objectives will be:
   i) Data in the database must be authorized, accurate, complete and timely. To ensure that this objective is achieved database controls must be in place.
   ii) The program used to prepare online output must work in authorized, accurate and complete manner. To assure standard package like SQL is used.
   iii) Only authorized users can access database. Access controls.

c) Users transmit output through e-mail. The sender must be known. Digital signatures provide the way to verifying the source and authenticity of the sender of the message.

2. Distribution Controls – ensure that only the correct persons receive the output.
i) Recipients' electronic addresses should be kept current.
ii) Access controls might be needed to be established over distribution lists
iii) Periodically, distribution lists might be checked, therefore, to see that only authorized addresses exist on the list
iv) Controls also must exist to ensure timely distribution of online output.

3. Communication Controls – they are established to reduce exposures from active attacks (e.g. message insertion, deletion and modification) and passive attacks (release of message contents)

4. Receipt Controls
i) Before the file is accepted, it should be scanned for viruses.
ii) Controls should be established to reject any message that exceeds a certain size

5. Review Controls – controls must be in place to ensure imp output is acted upon on a timely basis by intended recipients. In light of this concern, some e-mail systems will automatically notify a sender if recipients are unavailable to read their mail for the period. The operations audit trail might be used to record the time and data at which online output reports were accessed and the length of the time internal during which they were reviewed.

6. Disposition Controls – after online output is distributed to a terminal, it is difficult to exercise control over subsequent disposition of the output. For e.g. users might copy the output to a diskette. It also might be possible to keep some type of secure log to record he actions taken by employees in relation to confidential output.

7. Retention Controls
i) Only authorized persons should be allowed to access retained online output

ii) Backup and recovery controls must be established

8. **Deletion Controls** – when the useful life of online output is expired, it should be deleted. The utility might be executed to search for online output files whose retention date has expired and to then delete these files.

AUDIT TRAIL CONTROLS

Accounting Audit Trail

What output was presented to users, who receive the output, when output was received and what action were subsequently taken with the output.

If an erroneous data item is discovered in an organization's output the accounting audit trail also can be used to determine those users who might have relied on the output to make a decision. If the erroneous output has been place in a page on the Web, however, the situation is often problematic. The output might have been accessed by a large number of persons who are external to the organization, and it might be impossible to track all the people who have relied on the output. Therefore, the organizations that make output publicly available often place a disclaimer with the output notifying that they use the output at their own risk. Organizations might still want to notify the users who have obtained erroneous output to reduce losses of goodwill that may arise.

The audit trail can also be used to determine whether unauthorized users have gained access. In this light, periodically management could examine the audit trail to determine whether the contents of output provided to users reflect improper access or improper activities.

The decision should also be made on what output will be stored in the audit trail and the retention period that will apply to the different types of output.

Operations Audit Trail

Maintains the record of the resources consumed to produce the various types of output. It might record data that enables print times, response times, and display rates for output to be determined. This data can then be analyzed to determine whether an organization should continue to provide different types of output to users. It can also provide information that enables the organization to improve the timeliness of output production and reduce amount of resources consumed in predicting output.

EXISTENCE CONTROLS

Output can be lost or destroyed for a variety of reasons. In some cases recovery is simple to accomplish, in other cases it is difficult or impossible.

One factor that affects the ease with which batch output recovery can be accomplished is the availability of report files. Many computer systems donot write output directly to an output device, instead, they write output to a magnetic file, and the output is later dumped to the output device. This strategy called spooling allows more efficient use of output devices.

Second factor – if a stock report must be recovered, therefore, the prior values of different data items have to be retrieved. Some type of beforeimage or afterimage and time stamp for the data items must be kept.

A simple batch processing run in which master files are updated with the transaction files and prior versions of the master files are not overwritten. Recovery of output is straightforward.

OPERATIONS MANAGEMENT CONTROLS

INTRODUCTION

Operations Management is responsible for daily running of hardware and software facilities so that:

i) production application systems can accomplish their work, and

ii) development staff can design implement and maintain application systems.

COMPUTER OPERATIONS – directly support the day to day execution of wither test or production systems on the hardware /software platforms available three types of controls exists: 1) operational controls 2) scheduling controls 3) maintenance controls

1. **Operational controls** – those that prescribe the functions that either human operators or automated operations facilities must perform.
   - Operations controls prescribe the functions that *automated operations facilities (AOFs)* might have been implemented to start and stop programs according to a predetermined schedule.
   - Where human intervention is required in operations activities , the primary controls to be used is specification of and compliance with a set of standards procedures i.e. documentation and training. For e.g. having to recover from a disk crash could be a rare event. When this types of disaster occurs, however, correct actions by operates are essential to complete recovery they must have high-quality, documented procedure to follow
   - Traditional controls like separation of duties, effective supervision and rotation of duties also reduce the exposures associated with operator activities.
   - Where operations activities are automated, auditors must be concerned about the authenticity, accuracy and completeness of the automated operations. The following sorts of questions must be addressed:
     i) Who authorizes the design, implementation and maintenance of AOF parameters?
     ii) Are AOF parameters maintain in a secure file?
     iii) How are new or modified AOF parameters tested?
     iv) Is there ongoing monitoring of authenticity, accuracy and completeness of AOF operations?
     v) How well are AOF parameters documented?
     vi) Is an up-to-date copy of AOF parameters stored off site?

2. **Scheduling controls** – those that prescribe how jobs are to be scheduled on a hardware/software platform. They ensure that computers are used only for authorized purposes and that consumption of system resources is efficient.
   - Production system should run according to a predetermined schedule setup by applications project managers and the operations manager. The purpose of this schedule is to authorize use of HW and system software resources. In addition, where possible the schedule should seek to time the execution of application systems so conflicting resource demands are minimized.
   - AOFs enforce compliance with an authorized production schedule. Where AOFs are not used, however, the operations manager must monitor compliance with the production schedule. An OS will provide and audit trail of jobs executed on a machine, and this audit trail can then be checked against the authorized schedule.

3. **Maintenance controls** – those that prescribe how HW is to be maintained in goods working condition. Maintenance of computer is either preventive or remedial in mature.
   - Performance monitoring software should be used to prepare regular reports on HW reliability. The operations manager should also review maintenance reports prepared by maintenance engineers to evaluate the results.
   - Depending on the levels of exposures several basic controls can be exercised over maintenance engineers. Periodically, another engineer might be hired to evaluate the work of primary engineer.

NETWORK OPERATIONS

1. **Wide area network controls**
   - An important tool that operators use to manage a Wan is *network control terminal* that allows following functions to be performed:
     i) Starting and stopping lines and processes

ii) Monitoring network activity levels
iii) Renaming communications lines
iv) Generating system statistics
v) Increasing backup frequency
vi) Inquiring as to system status
vii) Transmitting system warning and status messages
viii) Examining data traversing a communication line

- Network control terminal also performs following functions with respect to individual devices:
  i) Starting up or closing down a terminal
  ii) Inquiring as to a terminal's status
  iii) Generating control totals for terminal devices such as ATMs or POS terminal
  iv) Sending and receiving terminal warnings
- It enables the communications software to check the authenticity of a terminal when it attempts to send or to receive messages.
- A network controls terminal can be used to access logs and to trace the passage of the transaction through the network to the point of its disappearance.
- For an asset safeguarding and data integrity perspective, several controls must be exercised over operator use of a network control terminal:
- Only senior operators who are well trained and have a sound employment history should perform network control functions:
  i) Network control functions should be separated and duties rotated on a regular basis.
  ii) The network control software must allow access controls to be enforces so that each operator is restricted to performing only certain functions.
  iii) The network control software must maintain a secure audit train of all operator activities
  iv) Documented standards and protocols must exist for network operators
  v) Operations management must regularly review network operator activities for compliance

2. Local area network controls

Operations management of LAN occurs via facilities provided on file servers. Following types of functions can be performed:

i) Available disk space on a file server can be monitored.
ii) Utilization activity and traffic patterns within the network can be monitored, this info. can allow operators to reconfigure the network to improve performance, identify users who are using network resources inappropriately. It may allow management to better plant network expansion to accommodate future needs.
iii) Level of corrupted data within the network can be monitored. Transmission media might have to be replaced or the network reconfigured to reduce noise and cross-talk on transmission media.
iv) Special network cards are often employed to connect workstations to a LAN.
v) A file server can be used to execute software that prevents, detects and removes viruses.

Other utilities and devices are also available to assist i.e. *cable scanners* can be used to identify shorts, breaks within transmission media.

DATA PREPARATION AND ENTRY

Historically, all source data for application systems were sent to a data preparation section for keying and verification before it was entered into a computer system. Nowadays, much more data is keyed into a microcomputer located close the point of data capture. Input controls discuss how source documents and input screens can be designed to facilitate keyboarding of source documents.

- Lightening in a keyboard area should be adequate without causing glare
- The environment must be neither too noisy nor too quiet.
- Layout of the work area should be uncluttered to facilitate the work flow.
- Training of keyboard operator
- Backup of both input data and data preparation and entry devices.

PRODUCTION CONTROL

1. Input / Output Control

Production control personnel have responsibility for ensuring that they accept input only from authorized parties, logging and receiving the input, safe custody of the input, timely submission of input to processing and safe retention of processed output. For control purposes production personnel are responsible for:

- ☞ Ensuring that output is prepared on timely basis.
- ☞ Basic quality assurance checks on any output received on behalf of outside parties.
- ☞ Safe custody of and dispatch of output

2. Job Scheduling Controls

Jobs can be started on one of the two ways. First, users can start jobs via commands given at terminal. Alternatively, jobs can be started using automated scheduling facilities. This approach is usually followed when the job performs work on behalf of many users or its resource consumption has major impact on other jobs.

3. Management of Service Level Agreements

- ♦ SLAs are prepared b/w users are the computer operations facility. They specify the response time from operations facility, level of maintenance support, the costs they will incur for services they use, and the penalties that will apply in the event that either users or the operations facility fail to meet the terms of the agreement.
- ♦ An important control is to have user complaints about service levels directed to the production control section. It should be handled by an independent party.
- ♦ Service line agreement contains:

Product/service	Product manager	Description	Availability
Response time	Reporting	User responsibility	ISD responsibility
Payment	Variations		

4. Transfer pricing / chargeout control

If computer operations facility uses a transfer pricing or chargeout system, the production control section often has responsibility for billing users, collecting receipts and following up on unpaid accounts. In this light production control personnel must carefully monitor chargeout system to ensure that charges are aphorized, accurate and complete and understandable by users.

5. Acquisition of Consumables – printer, paper, diskettes, magnetic tapes, stationary etc.

Production control personnel have responsibility for acquiring and managing consumable that the computer facility uses. They should ensure adequate stock is available, monitor the price and control its use.

FILE LIBRARY

File library function takes responsibility for the management of an organization's machine readable storage media.

1. Storage of storage media

To manage large no. of removable storage media effectively, usually some type of automated library system is needed. Such system records the following:

i) An identifier for each storage medium
ii) Place where each storage medium is located
iii) Name of person who has ultimate responsibility
iv) Name of person who currently has the storage medium
v) Persons authorized to access each storage medium
vi) Files stored on each medium
vii) Date when the storage medium was purchases
viii) Dates when contents of storage medium can be deleted.
ix) Dates when storage medium last released from library
x) Dates when storage medium last returned to library

2. Use of storage media

The extent of control exercise over user of storage media should depend on the criticality of data maintained on the media. File librarians should issue removable storage media in accordance with an authorized production schedule.

Care should be taken when multiple files are assigned to a single storage medium. Unless proper control exists, an application system reading one file might be able to enter another file and read it.

As the retention date of files expires, the files should be expunged from storage media. This procedure reduces the likelihood of sensitive data being exposed at some future time.

3. Maintenance and disposal of storage media

Storage media should not remain unused for long periods of time. Otherwise the risk of read/write error occurring with the media increases.

If backup must be stored for long periods, backup media should be retrieved, say, six months and backup files rewritten to another medium.

When storage medium become unreliable, it is best to discard them. Care should be taking to ensure that all sensitive data is removed from discarded media.

4. Location of storage media

Removable storage media are located either on site or off site, they should be located on site if they are intended primarily to support production running of application systems. They should be located offsite if they are intended for backup and recovery purposes.

In a mainframe environment, file librarians are responsible for managing the transport of removable storage media. Such movements should comply with backup schedules prepared by a team comprising security administrator, database administrator, application project managers, manager responsible for operations development, operations manger and file librarian.

DOCUMENTATION AND PROGRAM LIBRARY

Many types of documentation needed to support the IS function within an org. strategic and operational plans, application system documentation, system software and utility program documentation, data base documentation, operations manuals, user manuals and standards manuals, much of this documentation is now kept in automated form. System analysts use CASE tools to produce machine-readable versions of DFD and entity relationship model. Some software vendors now provide the documentation on optical disks (CD-ROM).

Documentation librarian's functions include:

1) ensuring that documentation is stored separately
2) ensuring that only authorized personnel gain access to documentation
3) ensuring that documentation is kept up-to-date
4) ensuring that adequate backup exists for documentation

CAPACITY PLANNING AND PERFORMANCE MONITORING

Operations management must continually monitor the performance of the HW/SW platform to ensure that systems are executing efficiently, acceptable response times or turnaround times are being achieved, and acceptable levels of uptime are occurring.

Operations management has responsibility for devising a plan for monitoring system performance, identifying the data tat must be captured to accomplish the plan, choosing the instruments needed to capture the data, and ensuring that the instruments are correctly implemented.

On the basis of performance monitoring statistics calculated, operations managers must make 3 decisions. First, they must evaluate whether the performance profiles indicate unauthorized activities might have occurred. Second, they must determine whether system performance is acceptable.

HELP DESK / TECHNICAL SUPPORT – typical functions include:

i) Acquisition of HW and SW on behalf of end users
ii) Assisting end users with HW and SW difficulties
iii) Training end users to use hardware, software and databases
iv) Answering end user queries

v) Monitoring technological developments and informing end users for developments that might be pertinent to them.

vi) Determining the source of problems with production systems and initiating corrective actions

vii) Informing end users of problems with hardware, software, or databases that could effect then

viii) Controlling the installation of hardware and software upgrade

For the help desk/technical support area to function effectively and efficiently there are two critical requirements:

First, competent and trust worthy personnel are essential, they must have high level of interpersonal skills so they can interact effectively with users.

Second, a problem management system that provides inventory, logging and reporting capabilities must be available to support the activities of the help desk. The system should also maintain a log of all activities undertaken relating to the difficulty reported or the advice requested. This log can be used to determine whether problems are occurring in a particular area.

MANAGEMENT OF OUTSOURCED OPERATIONS

1. **Financial Viability Of Outsourcing Vendor**
2. **Compliance With Outsourcing Contract's Terms And Conditions**
3. **Reliability Of Outsourcing Vendor's Controls**

   Two strategies might be followed. First, the outsourcing vendor might be required periodically to provide a third-party audit report attesting to the reliability of controls implemented by the vendor.

   Second, the outsourcing vendor might permit a review of its controls to be undertaken periodically by its clients internal and external auditors.

4. **Outsourcing Disaster Recovery Controls**

   An outsourcing contract should specify the disaster recovery controls that outsourcing vendor will have in place and working. These controls should be evaluated periodically. Client organization should develop their own disaster recovery procedures, however, in the event their outsourcing vendor experiences a disaster.

   An organization's security administrator should be responsible for the design and implementation of disaster recovery controls associated with an outsourcing contract. Operations management might be responsible for the day to day operations of these controls and adequacy of these controls.

EVALUATING ASSET SAFEGUARDING AND DATA INTEGRITY

MEASURES OF ASSETS SAFEGUARDING AND DATA INTEGRITY

To make a decision on how well assets are safeguarded, auditors need a measure of asset safeguarding. The measure they use is the expected loss that will occur if the asset is destroyed, stolen or used for unauthorized proposes. Similarly, to make a decision on how well data integrity is maintained, auditors need to measure data integrity for which they will depend on their audit objectives and the nature of the data item on which they focus. Three measurers they can use are:

a) the size of the dollar error that might exist and

b) the size of the quantity error that might exist and

c) the number of errors that might exist.

NATURE OF GLOBAL EVALUATION DECISION

When auditors made the global evaluation decision, they seek to determine the overall impact of individual control strengths and weaknesses on how well assets are safeguarded and how well data integrity is maintained. They make this decision at various stages during the conduct of audit:

a. after having undertaken preliminary audit work and gained an understanding of the control structure

b. after having undertaken tests on controls and

c. after having undertaken substantive tests

DETERMINANT OF JUDGMENT PROCESS

The determinants of auditor's judgment performance can be usefully grouped into four categories

i) The auditor's cognitive abilities, which are subject to various biases that can arise from the heuristics that auditors use to help them make judgment.

ii) The auditor's knowledge which has been developed on the basis of education, training and experience

iii) The environment in which the auditor must make his decision, which depends on factors like technology available to assist the auditor, the extent to which group judgment processes are used during the audit, the auditor's prior involvement with the audit and the extent to which the auditor will be held responsible

iv) The auditor's motivation, which will depend on factors like how accountable the auditor will be held for his work.

AUDIT TECHNOLOGY TO ASSISTS THE EVALUATION DECISION

1. **Control matrices –** in controls matrix, we list the exposures that can occur in the columns of the matrix and the controls we use to reduce expected losses from these exposures in the woes of the matrix. In the elements of the matrix, we might indicate, for e.g. how effectively a particular control reduces expected losses from a particular exposure.

2. **Deterministic models –** simply involve estimating the size of each error or loss and multiplying it by the number of times the error or loss has occurred, these models are most useful when errors and irregularities occur deterministically (program either makes the error or not). Even if errors or irregularities occur stochastically, the size of the error or loss can still be estimated on the basis of the most likely value of the error or loss or the extreme values of the error or loss

3. **Software reliability models –** use statistical technique to estimate the likelihood that an error will be discovered during some time period based on the pattern of past errors that have been discovered. Three types of models have been developed:

   Time-between-failures models are based on the assumption that the time b/w successive failures of the system will get longer as errors are removed from the system.

   Failure-count models are used to predict the no. of errors that are likely to occur during a time interval on the basis of the number of errors that occurred during previous time intervals.

   Fault-seeding models make estimated of the number of errors that exist in a system based on the number of seeded errors that are discovered during a testing process and the number of new errors that are discovered during the testing process.

4. **Engineering reliability models –** allow auditors to estimate the overall reliability of a system as a function of the individual components and individual internal control that makeup the system. They are based on three fundamental parameters:
   i) The probability that a process in the system will fail
   ii) The probability that a process will correctly signal an error or irregularity when one occurs,
   iii) The probability that the error or irregularity will be corrected when one occurs.

5. **Simulation models –** might be used to make the evaluation judgment. A program must be constructed to capture the important characteristics of the system to be evaluated, and the program must then be run to study the behaviour of the system it is intended to model. From the auditor's point of view, their focus will be the likely error or loss that can arise from errors or irregularities n the system that is being modeled by the simulation program.

6. **Expert systems –** are another means with the help of which the auditors can make the global evaluation judgement on whether a system safeguards assets and maintains data integrity. They provide auditors with insights in which control strengths and weaknesses compound and compensate to affect the overall reliability of the system.

   Perhaps the most important issue the auditors need to consider when using expert system to assist with the global evaluation judgment is the particular domain for which it has been developed. The performance of many expert systems is brittle if they are used outside a specialized domain for which they have been developed.

COST EFFECTIVE CONSIDERATIONS

1. Costs and benefits of controls

There are 5 costs associated with implementing and operating controls in a system:

a. initial setup cots that must be incurred to design and implement the controls
b. costs to execute the controls
c. costs to search for errors and irregularities when they are signaled, determine whether they exists and correct them when they are found
d. costs associated with errors and irregularities that are not discovered but not corrected; and
e. costs associated with maintaining the controls.

2. Controls in investment decision

The design, implementation, operating and maintenance of a controls system produce a stream of benefits and costs over its life. In this light, whether to establish a control system should be considered as a capital investment decision, thus, standard NPV criteria can be used to take the decision. Auditors will have to estimate the size of the benefits and costs during each period of the control system's life. In addition, they will have to estimate the discount rate the use. Unfortunately given the nature of a control system, estimating the appropriate discount rate to use might be difficult.

EVALUATING SYSTEM EFFECTIVENESS

OVERVIEW OF EFFECTIVENESS EVALUATION PROCESS

The purpose of evaluating system effectiveness is to determine how well a system meets its objectives. The evaluation involves six steps:

- Identify the objectives of the information system
- Select the measures to be used
- Identify the data sources
- Obtain values of these measures before the system was implemented
- Obtain values of these measures after the system was implemented
- Assess the system impact by comparing the above two values

A MODEL OF INFORMATION SYSTEM EFFECTIVENESS

To be able to evaluate system effectiveness and understand why a system us either effective or ineffective, auditors need a model of how the various factors that potentially impact system effectiveness are interrelated. One useful model imagines that the quality of the system and the quality of information it produces have an impact on user's perceptions about the usefulness of the system and the ease with which the system can be used. These two perceptions are also affected, however, by the users' beliefs about their abilities to use computer competently – their self-efficacy. User's perceptions about the usefulness and ease of use of the system in turn affect how the use the system – for e.g., the frequency with which they use the system and the ways they use the system. How they use the system then affects their performance in their organizational role and ultimately the overall performance of the organization. How they use the system also affect their satisfaction with it.

EVALUATING SYSTEM QUALITY

There are many characteristics of the hardware and software components of an IS that might effect users' perceptions of the usefulness and ease of use of the system. For e.g.

- Response time
- Reliability of the system
- Ease of interaction with the system
- Quality of documentation and help facilities
- Extent of integration with other systems.

The auditor might also need to evaluate factors that are somewhat opaque to users be nonetheless affect system quality for e.g.

- The extent to which the hardware platform is efficient,
- the extent to which the software platform has to be maintained,
- the operational efficiency of the system, and
- the extent to which the hardware software components are independent of one another so they can be adapted quickly in light of changing needs.

To assist the auditor to make a judgement about software effectiveness, they should examine follow attributes of software:

i) History of repair maintenance

ii) History of adaptive maintenance – adaptive maintenance occur due to two reasons. First, program designers might have formulated incorrect specification in first place. Second, user requirements might change.

iii) History of perfective maintenance – it is carried out to improve program resource consumption, to make the program execute more efficiently.

iv) Run-time resource consumption

EVALUATING INFORMATION QUALITY

There are several aspect of information quality – for e.g. authenticity, accuracy, completeness, timeliness and relevance. The importance of these characteristics will vary, depending on the nature of the system. For e.g. accuracy will be more important in an operational controls system and less important in a strategic planning.

The perceptions of these characteristics can also vary across users. For example one user might perceived some information to be more relevant that another user.

Auditors must recognize that different users might have different perceptions about the quality of information produced by a system. One person's perception of the world might not be the same as of another's

EVALUATING PERCEIVED USEFULNESS

Perceived usefulness is linked to whither users will ultimately gain rewards from their use of an IS and therefore the attitudes they have toward using the system. If their attitudes are favourable, they are likely to use the system more frequently and more effectively. Following items are valid to measure the perceived usefulness.

i) Users perceive that the IS enables them to increase their productivity
ii) Users perceive that the IS enables them to accomplish tasks more quickly
iii) Users perceive that the IS enables them to improve their job performance
iv) Users perceive the IS to be useful in their job

EVALUATING PERCEIVED EASE OF USE

Users will judge the ease of use of an IS in terms of the amount of effort they will have to expend to employ the functionality provided in the system.

i) Users perceive that it is easy for them to learn to operate the IS.
ii) Users perceive that they can interact with the system in a clear and understandable way
iii) Users perceive that interaction with the system is flexible
iv) Users perceive that they can quickly become skillful with the IS
v) Users perceive that the IS will be easy to use.

Both perceived usefulness and perceived ease of use would affect how users work with the system.

EVALUATING COMPUTER SELF-EFFICACY

It means "the judgment of one's ability to use a computer. It is an important variable in accounting for the likely effectiveness of an IS. It is not confined to straight forward skills like copying files and entering data into spreadsheets. Rather, it applies to broader tasks like using a spreadsheet effectively to undertake financial statement analysis. Computer self-efficacy is likely to affect users; perceptions of the usefulness and ease of use of an IS.

EVALUATING INFORMATION SYSTEM USE

Auditors must be careful when evaluating how Information systems are used:

First, they need to determine whether use of a system us voluntary or involuntary. If the use is voluntary,, auditors can build monitors into the system to determine how often the system us invoked by users to perform different tasks. Is use in involuntary (compelled), the auditors must the attempt to determine whether use is "real" or "apparent". If use is involuntary, the amount and frequency of use is not a good indicator of the effectiveness of IS.

Second, they need to examine the nature of the use made of an IS. For certain types of systems (e.g. DSS), it might be important to see that IS has produced fundamental changes in the ways users perform their jobs before auditors can judge the system to be effective.

Third, the auditors might need to determine who uses a system to determine its effectiveness. In some cases it might be best if users work directly with a system themselves. In other cases, if they use intermediaries (for some DSS) to work with the system on their behalf.

EVALUATING INDIVIDUAL IMPACT

Two important way that auditors can evaluate the effects of n IS on users are to examine *task accomplishment impacts* and *quality of working life impacts*. If the system improves *user's task accomplishment* it might also improve *quality of working life*.

1. **Task accomplishment impacts** – following are the measures that auditors can use to try to determine whether a user's task accomplishment has improved
   i) Decision accuracy
   ii) Time to make decision
   iii) Effectiveness of decision
   iv) Quality of product or service produced
   v) Customer satisfaction with product or service produced, and

vi) Time to undertake task

2. Quality of working life impacts

The factors that contribute to a high quality of working life are:

i) Adequate and fair compensation

ii) Safe and healthy working conditions

iii) Opportunity to use and develop human capabilities (providing autonomy)

iv) Opportunity for continued growth and security

v) Social integration in the work organization (allow interpersonal openness and encourage sense of community)

vi) Constitution in the work organization (personal privacy, free space)

vii) Social relevance of work life

If auditors use these factors to assess the impact of IS on the quality of working life of its users, they will encounter 2 problems. First, they will find that different users have different perceptions of what constitutes a high quality of working life. For eg some consider productivity perspective, some from a physical perspective and some wages consideration. Second, it is often difficult to find valid and reliable measurement instruments to assess the quality of working life.

Because of these problems, one approach auditors can adopt to asses the quality of working life is to use surrogate measures – that is absenteeism rate, strike rate, stoppage rate, grievance rate, turnover rate, accident rate, sick rate, theft rate etc.

EVALUATING INFORMATION SYSTEM SATISFACTION

It is widely believed that users will be satisfied with an IS that they deem to be effective. IS satisfaction measures address issues like:

i) User relationship with information system staff

ii) Level of IS training provided to users

iii) The quality if information provided by the system

iv) Reliability of the system

Substantial overlap exists b/w IS satisfaction and ease-of-use measures.

ORGANIZATIONAL IMPACT OF INFORMATION SYSTEM

1. Organizational effectiveness

To evaluate the organizational impact of an information system, auditors need to understand the goals on an organization. The overall effectiveness of an IS can then be evaluated in terms of how well it enables an organization to achieve its goals.

In selecting goals, the auditors have to take great care at the outset to reach a good understanding of the important stakeholders in the IS and the goals they have for the system.

2. Economic effectiveness

There are 4 steps that audits need to undertake to evaluate the economic effectiveness of an IS.

First, they need to identify the benefits associated with the information system. Both tangible and intangible benefits are likely to have occurred. Different stakeholders in the system are also likely to have experience different types of benefits.

Second, they need to identify the costs associated with the information system, as with benefits both tangible and intangible costs are likely to have occurred and the costs are likely differ across different stakeholder groups.

Third, the need to value the benefits and costs they have identified. This task can be difficult, especially when they are attempting to value intangible benefits and costs.

Forth, they need to discount the benefits can costs to obtain NPV for the investment in IS., the most difficult aspect is to determine the appropriate discount rate

EVALUATING SYSTEM EFFICIENCY

OBJECTIVE OF EVALUATING SYSTEM EFFICIENCY – there are 2 reasons why auditors might become involved in evaluating system efficiency.

First, management might ask them to evaluate an existing operational system to determine whether its performance can be improved, and

Second, management ask them to evaluate alternative systems that they are considering for purchase, lease, rental or development.

THE EVALUATION PROCESS

There are 8 major steps to be undertaken during the efficiency evaluation process:

1. **Formulate the objectives of the study** – boundaries of the system to be evaluated. Nature of performance indices that will be required.
2. **Prepare budget for evaluation**
3. **Define performance indices**
4. **Construct a workload model** – that is the representative of the real system workload.
5. **Construct a system (configuration) model**
6. **Run experiments** – to determine the values of performance indices
7. **Analyse results –** when evaluating efficiency, auditors hypothesize (assume) certain relationship between the values of the performance indices and the characteristics of workload and system models. When experiments have been run with changed parameters and values of the performance indices determined, the data can be analysed to determine whether the relationships hypothesized do, in fact, exists.
8. **Provide recommendations**

PERFORMANCE INDICES

Performance index is a measure of system efficiency. It expresses quantitatively how well a system achieves some type of efficiency criterion. There are 4 types of performance indices:

1. **Timeliness indices** – which measure how quickly a system is able to provide users with the output they require;
2. **Throughput indices** – which measure how mush work is dome by a system over a period of time, i.e. for central computer throughput is measure in MIPS
3. **Utilization indices** – which measure the proportion of time a system is busy; and
4. **Reliability indices** – which measure the availability of a system to process a user's workload. Percentage to time system is available for processing is called uptime and % to time system is not available for processing is called down time.

WORKLOAD MODELS

A system workload is the *set of resource demands or service demands* imposed on the system by the set of jobs or transactions that occur during a given time period.

Conceptually workload can be characterized as a matrix. The rows in the matrix are the set of jobs or transactions that occur for the time period and columns us the matrix are HW, SW and data resources belonging to the system or the services provided by the system. The elements of matrix are the amount of each resource or service demanded buys each job/transaction. System efficiency must be defined in terms of given workload.

Purpose of Workload models

1. Using real workload of the system for evaluation purposes could be too costly.
2. Real workload cannot be used if the system to be evaluated is not operational
3. Auditors might want to carry out sensitivity analysis when evaluating system efficiency. To examine system under varying workloads it might be easier to change the characteristics of workload model than the real workload.

Properties of Workload models

1. It should be representative of real workload
2. It should generate requests for services that are appropriate to the system or the components of the system under study.

SYSTEM DEVELOPMENT MANAGEMENT CONTROLS

APPROACHES TO AUDITING SYSTEM DEVELOPMENT

We might conduct three types of audits of the systems development process:

1. **Concurrent audit** – auditors are members of the system development team. They assist them in improving the quality of systems development for the specific system they are building and implementing.
2. **Post implementation review –** in which they evaluate a specific system after it has been implemented. The objective is to improve the quality of the systems development process in general and the specific system in particular.
3. **General audit –** auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to from an audit opinion about the management's assertion relating to financial statements or system effectiveness and efficiency.

An external auditor is more likely to undertake general audits rather than concurrent or post implementation audits of the systems development process. They may ask auditors to undertake a post implementation review if they believe they can provide cost-effective advice.

Both external and internal auditors must strive to preserve their independence. They should not conduct ex post reviews of any systems in which they were member of the systems development team. They cannot independently evaluate their own work. They can also protect their independence by ensuring that they have sufficient knowledge and skills to be able to form independent judgements about the quality of systems development work.

NORMATIVE MODELS OF SYSTEMS DEVELOPMENT PROCESS

1. SYSTEMS DEVELOPMENT LIFE CYCLE APPROACH

The SDLC approach emphasizes the importance of well-controlled work phases.

i) **Feasibility study** – applying cost benefit criteria to the proposed application
ii) **Information analysis** – determining user information requirements
iii) **System design** – designing the user interface, files to be used and information processing function to be performed by the system
iv) **Program development** – designing, coding, compiling, testing and documenting programs.
v) **Procedures and forms development** – designing and documenting system procedures and forms for the users of the system.
vi) **Acceptance testing –** final testing of the system and formal approval and acceptance by management and users.
vii) **Conversion** – changeover from the old system to new system.
viii) **Operating maintenance** – ongoing production running of the system and subsequent modification and maintenance in light of problems detected.

2. SOCIO TECHNICAL DESIGN APPROACH

This design approach seeks to optimize two systems jointly: (a) the technical system, in which the objective is to maximize task accomplishment; and (b) the social system, in which the objective is to maximize the quality of working life of system users.

Socio-technical design proponents argues that many problems arose because the SDLC model had inadequate procedures for dealing with the social system i.e. it did not adequately take into account the impact system might have on its users via a changes job or organizational structure design. In addition socio-technical design proponents argue that system development personnel were poorly trained in the social aspects of IS. They might affect a user's quality of working life.

3. POLITICAL APPROACH – emphasizes the importance of well-controlled work phases.

To study the history of organization and evaluate whether the designated system will leave existing power structure intact or changes are necessary.

In org, structure remains same, user participation in design is important to ensure congruence b/w system and organization.
However, design and implementation is difficult. Indeed, user participation might be counter productive because users feel they are being manipulated. **Or**
They might attempt to change the design to be congruent with their own political motive. Participation must be replaced by meaningful negotiations between designers and users where compromise is an accepted outcome

4. **SOFT SYSTEM APPROACH –** this approach is designed to assist decision makers to learn about and to better understand ill-structured problems. They called this approach "soft system methodology" (SSM) because it focuses on learning and innovation in a problem situation.

5. **PROTOTYPING APPROACH –** it includes developing an initial prototype system, gaining experience with the prototype, modifying the prototype in light of this experience and continuing to iterate through this cycle until an acceptable solution is found. High level programming languages are used because they facilitate rapid iteration through successive designs. The system can then be programmed in low level language.

   Using high level programming languages, end users can undertake their own development work independently of IS personnel. Auditors must be concerned about whether end users always have sufficient knowledge to design and implement high quality IS.

   Briefly prototype approach comprise of following steps:

   a. Elicit user requirements
   b. Design prototype
   c. Implement prototype
   d. Use prototype
   e. Build production system

6. **CONTINGENCY APPROACH –**They seek to identify factors that affect the effectiveness of different approaches.

EVALUATING MAJOR PHASES IN THE SYSTEM DEVELOPMENT PROCESS

Certain phases will always be present in the system development process, even though the conduct, timing and sequence of these phases might differ markedly across projects.

1) Problem/opportunity definition
2) Management of change process
3) Entry and feasibility assessment
4) Analysis of the existing system
5) Formulation of strategic requirements
6) Organizational and hob design
7) Information processing system design
8) Application software acquisition and development
9) Hardware/system software acquisition
10) Procedures development
11) Acceptance testing
12) Conversion
13) Operation and maintenance

1. Problem/opportunity definition

System can be developed to help:

   f. Resolve problem
   g. To take advantage of opportunities

The stakeholders must come to some understanding of the nature of the problem or opportunity they are addressing.

   i) Is the problem or opportunity well or ill structured?
   ii) Does it have implications for a small or large no. of people?
   iii) Will possible solutions have a large impact on the organizational structure and jobs?
   iv) Well new technology most likely be needed to support possible solutions?

Auditors have the following type of concerns:

i) If possible IS solutions will be material in terms of size or impact, have formal terms of reference prepared and approved by steering committee?

ii) If possible IS solutions will have major impact, what level of acceptance exists among stakeholders on the need for change?

iii) Do stakeholders agree on the definition of the problem or opportunity?

Auditors are concerned to see that the stakeholders have reached agreement on the problem or opportunity and that they have an understanding of the threats to asset safeguarding, data integrity, system effectiveness and system efficiency.

2. Management of change process

Management of change process run parallel to all other phases. The change process starts at the initial conception of the system and continues until the new system is running and the organization has adjusted to the new system.

It involves two major tasks project management and change facilitation:

i) *Project management* – involves budgeting, exception reporting, checkpoints and user signoffs.

ii) *Change facilitation* **–** aspects of system development becomes more critical as possible solutions are likely to have a greater impact on organizational structures and jobs. Management of change facilitation might also require that stakeholders undertake negotiation and compromise.

3. Entry and feasibility assessment

The purpose of this phase is to obtain a commitment to change and to evaluate whether cost-effective solutions are available to address the problem or opportunity.

i) *Technical feasibility* – is the available technology sufficient to support the proposed project? Can the technology be acquired or develop?

ii) *Operational feasibility* – can the input data be collected for the system? Is the output useable?

iii) *Economic feasibility* – do the benefits of the system exceed the costs?

iv) *Behavioral feasibility* – what impact will the system have on the user's quality of working life?

4. Analysis of the existing system – for e.g. how employees are rewarded under the current system to determine the likely impact the proposed system will have on these rewards. Any redistribution of rewards that arises as system as a result of the new system might have to be negotiated carefully. Analysis of current system includes 2 major tasks:

a) Studying the existing organizational history structure and culture- to gain an understanding of the social and task systems in place, the ways these systems are coupled, and the willingness of stakeholders to change.

b) Studying the existing product and information flows – is important for three reasons:

i. sometimes the design of the proposed system will be based preliminary on current product and information flows. The new system is not intended to be a departure from the status quo.

ii. Designers might need to understand the strengths and weaknesses of the existing product and information flows to determine the new system requirements.

iii. Third, a good understanding of existing IS might be required to assess the extent of change needed to implement and operate the new system.

Structured analysis (top down approach) and object oriented analysis are popular methods of analyzing and documenting product and information flows.

5. Formulation of strategic requirements – specify the overall goals and objectives the system must accomplish.

- ☞ Many system failures can be attributed to inadequate performance of this activity.
- ☞ If the strategic requirements for a system are clear, stakeholders are better placed to consider and evaluate alternative designs.
- ☞ Auditors should be concerned to see that system designers recognize the importance of articulating strategic requirements for the quality of subsequent deign work.

6. Organizational and job design

The design of organization structures and job can be a complex activity. If the auditors assess that a proposed system will impact organizational structures and jobs, they would be concerned to see the systems

development team obtained high-quality advice from someone skilled in organizational theory and practice. They would seek evidence on:

- whether personnel assigned responsibility for organizational structure and job design contained representatives of stakeholders group,
- how the design tasks undertaken,
- the processed used to resolve conflict and uncertainties and
- the level of consensus achieved in relation to the designs finally chosen

If the auditor concludes that these types of issues have been resolved satisfactorily, they can reduce the level of control risks and then the substantive testing.

7. Information processing system design – comprise of six activities:

a. Elicitation of detailed requirements – what information it must provide, the data that must be captured to produce this information, and the transformation that must be undertaken on the data to transform it into information. There are 2 approaches:

i. Ask the stakeholders what they require

ii. Discover the requirements through analysis and experimentation

If there is high level of uncertainty then soft-system and prototyping approaches are used.

b. Design of the data/information flow – designers must determine the following:

i) The flow of data and information and the transformation (conversion) points

ii) The frequency and timing of the data and information flows; and

iii) The extent to which data and information flows will be formalized

Failure to produce a high quality design for the data/information flow can seriously undermine a system. For e.g. poor timing decision can result in out-of-date data being captured, poor choices about information flows could mean information is directed to the wrong decision makers.

c. Design of the database – involves determining its scope and structure. Scope of database range from local to global. Four activities in respect of structure must be undertaken:

i) Conceptual modelling – describe the application domain via entities, attributes of these entities, relationship b/w these entities and static and dynamic constraints on these entities.

ii) Data modelling – conceptual model must be translated into data model so they can be accessed and manipulated by means of both high-level and low-level programming languages. E.g. entity relationship model translated into relational model.

iii) Storage structure design

iv) Physical layout design

d. Design of user interface – involves determining the ways in which users will interact with a system. Some elements are considered follow:

i) Source documents to capture raw data

ii) Hardcopy output reports

iii) Screen layouts for dedicated source-document input

iv) Inquiry screens for data interrogation

v) Graphic and color displays

vi) Voice output to guide users

vii) Icons for pectoral representation of output

viii) Command languages for DSS

ix) Interrogation languages for the database.

e. Physical Design – process involves breaking up the logical design into units, which in turn can be decomposed further into implementation units such as program and modules.

During physical design auditors primary concerns will be with the effectiveness and efficiency issues.

f. Design Of Hardware / System Software Platform – in some cases the new system requires hardware and system software not currently available in the organization. The new hardware/software platform required to support the application system will have to be designed. Different HW and system SW platform must be able to communicate with each other.

8. Application software acquisition and development

In some cases generalized software can be purchases to perform all or some functions. These packages have to be configured and perhaps modified and adapted. In other cases the system might exist in a prototype form at the conclusion of the design phase. Work might be undertaken to tune the prototype so it runs more efficiently or to write the prototype in an other programming language that will execute more efficiently.

Auditors might have several concerns during the application software acquisition and development phase. If application system is acquired, they should be concerned about the adequacy of requirement specification provided to vendors, the quality of the procedures used to evaluate the software tendered in terms of such factors as functionality, accuracy, and completeness, quality of documentation, vendor stability and support, and the nature of the terms and conditions in the contract exchanged with the vendor.

9. Hardware/system software acquisition

Request for proposal must be prepared. Vendor's submissions must be evaluated and a final selection made. Request for proposal should document transaction volumes, database sizes, turnaround and response time requirements.

Auditor should seek evidence on whether simulation models were developed to evaluate the merits of different vendor submissions against the response time requirements specified in the request for proposal.

10. Procedures development

What needs to be done should be clearly specified. It involves 4 major tasks

i) Design of procedures – they must be matched with the job/ tasks design

ii) Testing of procedures – test the adequacy of the procedures design.

iii) Implementation of procedures – in the way that people have to change their behaviour when a new system is implemented

iv) Documentation of procedures – formal documentation in procedure manual

11. Acceptance testing

Errors and deficiencies can exists in the software, user interface, procedures manuals, job design, organizational structure design and so on. Acceptance testing is done to identify these errors or deficiencies. There are 4 major types of acceptance testing:

a. Program testing – done by programmers for accuracy, completeness and efficiency

b. System testing – testing the entire system to ensure interfaces b/w various programs and subsystems working properly.

c. User testing – users must test the entire system including org. structure design, job design, system interfaces, programs and procedures etc.

d. Quality assurance testing – quality assurance group is responsible for ensuring the system complies with all standards adopted by org.

Auditors should ask following types of questions:

- ☞ How the testing process planned?
- ☞ How were test data planned?
- ☞ What test data used?
- ☞ What actions were taken as a result of error or deficiencies identified?
- ☞ What subsequent modification to test data?

12. Conversion

In case replacement of old system transition must be made from an existing system. Conversion requires users to adopt new behaviours. Type of conversion:

a. ***Abrupt / direct conversion*** – the new system us introduced and start operation and the old system is excluded from operation at a time.

b. ***Phases conversion*** – where only a few department/branch offices at a time are converted. It allows a gradual implementation process to take place in an organization.

c. ***Parallel conversion*** – where both the old and the new system are operated until the project development team and end user management agree to switch over to the new system. The operations and results of both systems are compared and evaluated.

d. ***Pilot conversion*** – where one department serves as a test basis. A new system can be tried out at this site until developers feel it can be implemented through out the organization.

Changeover can involve 4 major activities:

i) Personnel training
ii) Installation of new hardware and software and testing
iii) Conversion of files and programs
iv) Scheduling of operations and test running

Auditors often pay special attention to several aspects of conversion phase:

i. If substantial disruption is likely to occur, asset safeguarding, data integrity, system effectiveness, and system efficiency are at risk. For e.g. a programmer could take adv. Of a situation in which managers have insufficient time to review program modifications to install unauthorized code. Likewise, a data-entry clerk could introduce unauthorized transactions into the system when large backlogs of input exist and many data-entry errors have to be corrected.

ii. Conversion can be a time when tempers fray (conflict) and users become severely disillusioned (disheartened) with the system. As a result they might begin to undermine implementation efforts.

iii. Controls to endure asset safeguarding, data integrity, system effectiveness and system efficiency must be designed at conversion phase.

13. Operation and maintenance

The new system is run as a production system. In addition, periodically it is modified to better meet its objectives. In light of production experience with the system, three types of changes can be undertaken:

i) *Repair maintenance* – logical errors are corrected

ii) *Adaptive maintenance* – modification due to changes in system requirements

iii) *Perfective maintenance* – to improve performance efficiency.

Repair and perfective maintenance occur early in life of system. Adaptive maintenance occurs at later stages.

TOP MANAGEMENT CONTROLS

Auditors evaluate top management by examining how well they perform 4 major functions:

1) Planning – determining the goals of the IS function and the merits of achieving these goals;
2) Organizing – gathering, allocating and coordinating the resources needed to accomplish the goals;
3) Leading – motivating, guiding and communicating with personnel; and
4) Controlling – comparing actual performance with the planned performance as a basis for taking any corrective actions that are needed.

EVALUATING PLANNING FUNCTION

Top management is responsible for preparing a master plan, which contain both long run strategic plan and short run operational plan. Preparing plan involves three tasks:

- ☞ Recognizing problems and opportunities
- ☞ Identifying resources needed
- ☞ Formulating strategies for acquiring the needed resources

Auditors must ensure that management has formulated a high quality IS plan appropriate to the needs of the organization.

1. Types of plans

i) Strategic plan – contents of strategic plan typically includes the following:

a. Current information assessment
b. Strategic directions – future information services to be provided
c. Development strategy – vision statement, future applications

ii) Operational plan

a. Progress report

b. Initiatives to be undertaken – system to be developed, HW/SW platform changes, personnel resource acquisition.

c. Implementation schedule

2. Need for a contingency approach to planning

IS planning needs will vary depending upon such factors as:

- The importance of existing IS
- The importance of proposed IS
- The extent to which IS bas been integrated into daily operations, and
- The extent to which IT has been diffused throughout an organization

3. Role of steering committee – the IS steering committee should take ultimate responsibility for IS planning. The functions and makeup of the steering committee should vary depending upon how critical IS are to the success of the organization. For e.g. in strategic organizations steering committee should be chaired by Chief Executive.

EVALUATING THE ORGANIZATION FUNCTION

The organization function gathers, allocates and structures resources to enable these goals and objectives to be achieved.

1. Resourcing the Information Systems Function – major responsibility of top management is to acquire the resources (HE, SW, personnel, finances) needed to accomplish the goals and objectives. Detailed requirements must be set and request for proposal must be evaluated, contracts must be exchanged, the HW and SW must be installed and tested.

2. Staffing the IS Function – the effectiveness of the IS function depends on the quality of its staff.

- The staff remains up-to-date and motivated in their jobs.
- Staffing IS involves three major activities:

a. Acquisition of personnel – top management must carefully evaluate the integrity and capabilities of job applicants through interviews, references, resumes etc.

b. Personnel development – training and continuing education. Staff reviews should be carried out to identify for strengths and weaknesses.

c. Personnel termination – whether voluntary or involuntary following control procedures to be followed:

i. Prepare checklist of control procedures to ensure keys and ID badges are recovered, passwords are cancelled, distribution lists are changed any equipment issued is returned.

ii. Exit interviews should be given

3. Centralization Verses Decentralization Of IS Function

When deciding whether to centralize or decentralize depends on decision that have to be made with respect to ***control*** over IS resources, ***location*** of IS resources, and the IS ***function*** to be performed at different sites.

4. Internal Organization of Information Systems Function

Auditor is concerned about two matters in terms of the ways IS jobs are defined.

First, the responsibilities of each job position must be clear and they understand their duties, errors and irregularities.

Second, to the extent possible, the jobs performed within the IS function should preserve separation of duties.

5. Location of information systems function

Information System	*Location*
Strategic	separate IS dept. that takes org. wide responsibility for IS function
Support role	IS functions dispersed to user groups

EVALUATING THE LEADING FUNCTION

The purpose of leading function is to achieve harmony of objectives i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them. How can be evaluate how well top management performs the leading function? We must have a basic understanding of 3 areas fundamental to effective leadership.

a. How to motivate subordinates – contingency theory is the best one to tell.
b. Match leadership styles with the IS personnel and their job
c. Effectively communication with subordinates

EVALUATING CONTROLLING FUNCTION

The controlling function involves determining when the actual activities of the IS function deviate from the planned activities.

1. Overall control of the Information System Function

In this regard, top management asks 2 questions:

i) How much should the organization be spending on the IS function?

Here managers should look to industry averages to determine how much they should be spending on the IS function. This strategy called benchmarking. Benchmarking can be problematic –

First, it reflects the reactive rather than proactive stance by top management.

Second, organizations might need to deviate purposefully from industry averages. High level of spending may be required to catch up with industry norms.

Third, spending on the IS function is not tied to the overall corporate strategy.

ii) Is the organization getting value for money from its IS function?

Individual IS function can be subjected to a post audit to evaluate whether their benefits exceed their costs.

2. Technology Diffusion and Control of the Information Systems Function

Management's ability to exercise controls over IS function depends on the ways different technologies have diffused throughout the organization. Different controls need to be implemented at different stages: initiation, contagion (infection), control (computer moves up to separate user area), and integration (data processing become a separate functional area.

3. Control of Information System Activities

Top management should seek to achieve control over the activities undertaken through the establishment and enforcement of ***policies and standards***. If the distribution of IS resources within organization is an important goal, policies will be needed to provide guidance on the types of hardware and software that can be purchased to ensure compatibility among systems. Following standards may be established:

a. Methods standards – uniform practices and procedures e.g. how analysis, design and programming practices to be carried out.
b. Performance standards – resource usage expected form undertaking IS activities
c. Documentation standards – activities undertaken need to be documented
d. Project control standards – the major check-points at which reviews to be undertaken
e. Post audit standards – makeup of review team, activities they should undertake

4. Controls over the Users of Information System Services

Users of computer services can be controlled by implementing zero based budgeting or transfer price (chargeout) scheme.

If top management choose to controls users via a transfer pricing or chargeout scheme, two decisions must be made.

First, they must determine how they wish to view the providers of IS services:

a. Cost centre – goal of recouping cost
b. Profits centre – goal of making profit
c. Investment centre – foal of making an acceptable return on these investments

d. Hybrid centre – different activities have different goals (any of the above)

Second, a specific transfer price or charge must be determined:

a. Allocated cost – cost charged on the basis of proportion of services consumed
b. Standard cost
c. Dual price
d. Negotiate price
e. Market price

The IS auditor must evaluate whether the top management's choice of control over users of IS services is likely to be effective. Following factors need to be considered:

- Is the organization trying to simulate innovation among IS services and constrain consumption of services?
- What level of accountability of IS services has been assigned to users?
- What level of maturity has the organization attained with respect to IS services?

CONCURRENT AUDITING TECHNIQUES

BASIC NATURE OF CONCURRENT AUDITING TECHNIQUES

Concurrent auditing techniques are used to collect audit evidence at the same time as an application system undertakes processing of its production data. They comprise two basic components:

i) ***First***, special audit modules are embedded in application systems or systems software to collect, process, and print audit evidence.

ii) ***Second***, in some cases, special audit records are used to store the audit evidence collected.

If concurrent auditing techniques identify a critical error or irregularity, they can notify auditors immediately by transmitting the audit evidence to a printer or screen that auditors should examine continuously. Alternatively, the evidence can be stored and printed or displayed at a later time.

NEED FOR CONCURRENT AUDITING TECHNIQUES

Five factors have motivated the use of concurrent auditing techniques.

1. **Disappearing of paper based audit trail -** Paper-based audit trail in application systems is progressively disappearing. Concurrent auditing techniques provide a way for auditors to capture the evidence that previously existed in this paper-based audit trail.
2. **Continuous monitoring required by advanced systems –** Errors or irregularities in advanced computer systems can propagate quickly to other systems and cause material losses. Concurrent auditing techniques allow auditors to monitor these systems on a timely basis.
3. **Increased difficulty of performing transaction walkthroughs in advanced computer –**Concurrent auditing techniques provide a means of tracing transactions as they follow different execution paths in an application system.
4. **Presence of entropy in systems –** which is their tendency to move toward internal disorder and eventual collapse. Concurrent auditing techniques provide early warning of the presence of and effects of entropy in application systems.
5. **Problems posed by outsourced and distributed information systems** for auditors because it is difficult for them to be physically present at information systems facilities to gather evidence. The **embedded** audit routines used with concurrent auditing techniques provide a way of collecting audit evidence when application system processing is carried out at remote locations.
6. **Problems posed by Inter-organizational Information Systems –** many organizations must rely on the **quality** of data processing carried out in other organizations to achieve assets safeguarding, data integrity, system effectiveness, system effectiveness and system efficiency objectives. For e.g. in an EDI errors or irregularities on one organization's IS can propagate to another organization's IS.

   Concurrent audit techniques can be used to monitor the quality of information received from other organizations. Auditors might use this technique in coordination with auditors of other organizations to monitor the quality of overall IS.

TYPES OF CONCURRENT AUDITING TECHNIQUES

1. Integrated test facility

Integrated test facility (ITF) is a concurrent auditing technique that involves establishing a dummy entity on an application system's files and processing audit test data against this dummy entity. In this way auditors can verify the application system's processing authenticity, accuracy, and completeness.

The **test data** used with ITF might be l*ive production transactions* that are tagged so the application system knows they must also be processed against the dummy entity. Alternatively, the *test data used could be designed specifically* by auditors according to a test plan and submitted as part of the normal production data for the application system. This approach makes more complete coverage of the execution paths in the application system to be tested.

The presence of ITF transactions in an application system affects the results obtained—for example, the control totals produced by the application system. Auditors can inform users that output has been affected by ITF transactions. Alternatively, they can try to remove their effects in some way. For example, auditors can modify the application system so that it does not include the effects of ITF transactions in any output it produces.

2. Snapshot

The snapshot concurrent auditing technique involves having embedded audit modules take pictures of a transaction as it flows through various points in an application system. The snapshots are either printed immediately or written to a file for later printing. Auditors must determine where they want to place the snapshot points in an application system, which transactions will be subject to snapshot, and how and when the snapshot data will be presented for audit evaluation purposes.

A modification to the snapshot technique is the extended record technique. Whereas snapshot writes a record for each snapshot point, the extended record technique appends data for each snapshot point to a single record. All the data relating to a transaction is kept, therefore, in the one place.

3. System control audit review file (SCARF)

The system control audit review file (SCARF) concurrent auditing technique involves embedding audit modules in an application system to provide continuous monitoring of a system's transactions. These audit modules are placed at predetermined points to gather information about transactions with in the system that auditors deem to be material. The information collected is written onto a special audit file.

The data collected via these routines includes errors and irregularities, policy and procedural variances, system exceptions, statistical samples, and snapshots and extended records. It is written to a special SCARF file for immediate or subsequent audit evaluation.

4. Continuous and Intermittent Simulation (CIS)

The continuous and intermittent simulation (CIS) concurrent auditing technique can be used whenever application systems use a database management system. Transactions that are of interest to auditors are trapped by the database management system and passed to CIS. CIS then replicates the application system's processing, and the two sets of results are compared. If CIS's results differ from the application system's results, data about the discrepancy is written to a special audit file. If the discrepancies are material. CIS can instruct the database management system not to perform the updates to the database on behalf of the application system.

IMPLEMENTING CONCURRENT AUDITING TECHNIQUES

When auditors implement concurrent auditing techniques, they should follow the same steps necessary to achieve any well-implemented system. Auditors must:

Perform a feasibility study:

a) Seek the support of persons who will be affected by use of concurrent auditing techniques:

b) Ensure that they have sufficient expertise to develop, implement, operate, and maintain concurrent auditing techniques effectively and efficiently:

c) Ensure that they have the commitment of key stakeholders including management, information systems staff and application system users:

d) Make the necessary technical decisions;

e) Plan the design and implementation:

f) implement and test the techniques: and

g) Carry out a post audit of costs and benefits after concurrent auditing techniques have been used for some time.

STRENGTHS / LIMITATIONS OF CONCURRENT AUDITING TECHNIQUES

The major strengths of concurrent auditing techniques are that they provide a

a) viable alternative to ex post auditing and auditing around the computer,

b) surprise test capability for auditors

c) test vehicle for information system staff, and

d) training vehicle for new users.

Surveys of audit use of concurrent auditing techniques indicate limited but stable use over many years. In addition, these surveys have found that concurrent auditing techniques are more likely to be used if:

a) The audit is conducted by internal auditors instead of external auditors

b) Auditors are involved in the development work associated with a new application system

c) Auditors are employing other types of CAAT, and

d) The incidence of automatically generated transactions in application systems goes up.

The major limitations of concurrent auditing techniques are:

a) the costs of developing, implementing, operating and maintaining them can be high.

b) they are unlikely to be used effectively and efficiently unless auditors have substantial knowledge of and experience with IS auditing; and

c) they are unlikely to be effective unless they are implemented in application system that are relatively stable.

AUDIT SOFTWARE

INTRODUCTION

Various types of software can be used to assist auditors in evidence collection. Some can be *purchased off the shelf*. Others must be *developed specifically* to address audit needs.

GENERALIZED AUDIT SOFTWARE

1. Motivations For Using Generalized Audit Software Development

Generalized audit software is a major tool that auditors can use to collect evidence on the quality of application systems. Generalized audit software provides a means to gain access to and manipulate data maintained on computer storage media. It was developed to allow auditors to:

a) undertake their evidence-collection work in a variety of hardware/software environments,

b) develop an audit capability quickly, and

c) Minimize the technical knowledge auditors need to be able to retrieve data from and manipulate data in computer-based information systems.

2. Functional Capabilities of Generalized Audit Software

Generalized audit software provides the following major sets of functions:

a) file access functions that permit different types of file structures, record formats, and data formats to be read;
b) file reorganization functions that allow files to be sorted and merged;
c) selection functions to extract data that satisfies certain conditional tests;
d) statistical functions to allow sampling to be undertaken and the results of sampling to be evaluated;
e) arithmetic functions to enable computations to be performed on data;
f) stratification and frequency analysis functions to allow data to be categorized and summarized in different ways;
g) file creation and updating functions to allow work files to be created and updated; and
h) Reporting functions to allow results to be formatted and output in flexible ways.

3. Audit Tasks That Can Be Accomplished Using Generalized Audit Software

The functional capabilities of generalized audit software can be used to accomplish four major audit tasks:

a) examine the existence, accuracy, completeness, consistency, and timeliness of data maintained on computer storage media;
b) examine the quality of processes embedded within an application system:
c) examine the existence of the entities the data purports to represent by facilitating physical observation and counting of these entities via statistical sampling;
d) undertake analytical review to monitor key audit indicators such as trends in working capital ratios over time.

4. Functional Limitations Of Generalized Audit Software - Generalized audit software has three functional limitations:

a) It permits auditors to undertake only ex post auditing and not concurrent auditing. Concurrent auditing techniques are discussed in Chapter 18;

b) It can perform only limited tests to verify the authenticity, accuracy and completeness of processing logic. As a result exceptional conditions can not tested accurately and completely. To overcome this problem test data must be designed specifically;

c) Auditors must be concerned with whether application system designed appropriately to accommodate change. Generalized audit software can gives only little evidence on an application system's capability to accommodate change.

5. Accessing Data with Generalized Audit Software

Sometimes auditors will want to use generalized audit software to access data maintained on another machine. There are several ways auditors can transfer data from the other machine to the machine on which the generalized audit software package resides. The file can be written to a cartridge, tape, or diskette that can be read by the machine on which the generalized audit software package resides; the data can be transferred via a modem and a file transfer utility; or the data can be transferred via a gateway to a local area network to which the machine where the generalized audit software resides is connected.

6. Managing a Generalized Audit Software Application

Generalized audit software applications must be managed properly like the development and implementation of any piece of software. The following phases should be managed carefully:

a) feasibility analysis and planning for the generalized audit software application;

b) design of the generalized audit software application;

c) coding and testing of the generalized audit software application; and

d) operation, evaluation, and documentation of the results obtained from the generalized audit software application.

INDUSTRY SPECIFIC AUDIT SOFTWARE

Industry-specific audit software is audit software that has been designed to provide high-level commands that invoke common audit functions needed within a particular industry. It might run only on a limited set of hardware/software platforms. Moreover, it might have been developed to access data maintained by a specific application package that is used widely within the industry.

HIGH LEVEL LANGUAGES

Auditors might sometimes use high-level languages, such as fourth-generation programming languages and statistical software, to gain access to data and manipulate it. In some cases, fourth-generation languages could be more user friendly and better supported than generalized audit software. They might also perform functions that cannot be performed using generalized audit software. Statistical software might be used because it provides more powerful statistical functions than those provided in generalized audit software.

UTILITY SOFTWARE

Utility software is software that performs fairly specific functions that are needed frequently, often by a large number of users, during the operation of computer systems. Auditors can use utility software to:

a) facilitate assessment of security and integrity,
b) facilitate gaining an understanding of an application system,
c) assess data quality,

d) assess program quality,
e) facilitate program development, and
f) facilitate assessing operational efficiency.

EXPERT SYSTEMS

Expert systems are programs that encapsulate the knowledge that human experts have about a particular domain and possess capabilities to reproduce this knowledge when presented with a particular problem. They have four major components:

a) *knowledge base* that contains facts about the domain of interest and rules that experts use to solve problems in the domain;

b) an *inference engine* that uses the knowledge base to solve particular problems presented to the expert system. It employs some type of logic to establish interrelationship among facts and rules to reach a conclusion about a problem in the domain of interest;

c) a *tutorial component or explanation facility* to provide information to users about a line of reasoning used to reach a particular conclusion: and

d) a *knowledge acquisition component* that can be used to elicit new information about the domain so that expert system can progressively expand its capabilities.

Type of Audit Expert System

Audit expert systems have been developed to assist with *risk analysis*, *internal control evaluation*, *audit program planning* and *provision of advice on various technical aspects* of the audit (such as the adequacy of doubtful debts provision).

NEURAL NETWORK

Neural network software has been designed to function like neurons in the brain. It is used primarily for *pattern recognition*, *learning*, and *classification* purposes. For example, it can be used to recognize patterns in data that manifest fraud has occurred. Neural networks are "trained" by presenting them with a large number of cases where the outputs (or results) for a given set of inputs are known. The network learns by adjusting internal weights among its components until it can predict the output based on the input pattern.

SPECIALIZED AUDIT SOFTWARE

Specialized audit software is software written in a procedure-oriented or problem-oriented language to fulfill a specific set of audit tasks. The software might have extensive functionality but it has been developed for specific audit users lo achieve specific audit goals. Specialized audit software can be developed in three ways:

a) First, auditors can take total responsibility for developing and implementing the software themselves.

b) Second, internal auditors can ask programmers in their own organization to develop and implement the software.

c) Third, auditors could ask an outside software vendor to prepare the software.

Whatever the approach used, auditors must exercise careful control over the development and implementation process to ensure that the software meets their needs and the integrity of the software is preserved.

OTHER AUDIT SOFTWARE

Over the years, other types of audit software have been developed. For example, software lies been developed to simulate the operations of internal control systems, to generate questions to elicit internal control weaknesses, to allow description of an internal control system and questioning about the state of the internal control system, and to represent the complex interrelationships (hat sometimes exist between internal controls so system vulnerabilities can be assessed. Much of this software is experimental in nature. Nevertheless, auditors should be aware of it so they can obtain insights that might improve their audit practice.

Whenever auditors use audit software for evidence-collection purposes, they should evaluate the level of control they are able to exercise over the software. To the extent that the software is controlled by another party or auditors must rely on another party to execute the software, they run the risk of the integrity of the software or the results produced by the software being undermined either intentionally or unintentionally. Auditors should seek to maintain a library of audit software that can controls and execute themselves.

QUALITY ASSURANCE MANAGEMENT CONTROLS

INTRODUCTION

Quality Assurance (QA) management involves ensuring that the information systems produced by the information systems function achieve certain quality goals and that development, implementation, operation and maintenance of information systems comply with a set of quality standards.

MOTIVATIONS TOWARD THE QA ROLE

There are six reasons why the information systems QA role has emerged in many organizations:

a) Increasingly organizations are producing safely-critical systems i.e. air traffic controls, weapon guidance system. Errors in theses system can be devastating;

b) Users are becoming more demanding in terms of the quality of the software they employ to undertake their work. Otherwise their customer will switch to competitors about the quality of software;

c) organizations are looking for pioneering and innovative applications for software in an attempt to gain a competitive advantage;

d) organizations are becoming increasingly concerned about their liabilities if they produce and sell defective software;

e) poor control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied customers;

f) Improving the quality of software is part of a worldwide trend among organizations to improve the quality of the goods and services they sell. TQM now a major driving force in many organizations because of their need to compete effectively in international market places.

QA FUNCTIONS

QA personnel perform a monitoring role for management to ensure that:

a) Quality goals are established and understood clearly by all stakeholders and

b) Compliance occurs with the standards that are in place to attain quality information system

1. Developing quality goals

The first function of QA personnel is to develop quality goals for the information systems function overall and to assist in the development of quality goals for specific information systems. Following problems arise:

a) Obtaining consensus on quality goals can be difficult because different stakeholders have differing perspectives on quality. For programmers quality goal is well structuring of program code, and for top management better market place.

b) Quality goals might need to vary across information systems and at times quality goals may conflict with one another. In safety critical system accuracy and completeness may be of paramount objectives, in strategic planning timely reporting could override data accuracy and completeness.

When formulating the quality goals for specific IS, QA personnel must take care to ensure that specific goals are not in conflict with the overall goals of the organization.

2. Developing, promulgating, and maintaining standards for information systems function

Standards are the backbone of planning and control activities in the information systems function. QA personnel are in the best position to be responsible for standards because:

- they should be the most knowledgeable about standards,
- They understand the potential impact that standards may have on their own activities.
- they should be perceived as independent, and
- they have incentives to keep standards

The software Engineering institute has developed a Capability maturity modeling (CMM) that defines five levels of organizational maturity and the software quality processes associated with each of theses levels. **Same as maturity model in COBIT**

3. Monitoring compliance with QA standards

The third function of QA personnel is to monitor compliance with standards of two types. Monitoring must be undertaken in terms of *general* standards that govern the overall information systems function and *specific* standards that govern a particular information system.

When compliance failures occur with general standards, QA personnel should seek to understand the reasons for the failure so they can advice management. Such reasons could motivate reconsideration of standards. Non compliance could reflect a breakdown in a process, in which case corrective action will be needed.

QA personnel should also consider the consequences of compliance failure and should consider appropriate corrective actions.

4. Identifying areas for improvement

The fourth function of QA personnel is to identify areas for improvement. Identifying areas for improvement should be part of an ongoing process that leads to higher-quality information systems being produced. QA personnel should make recommendations for improvement based on facts rather than intuition or experience.

QA personnel should have responsibility for identifying areas for improvement due to the same factors as given in point (2)

5. Reporting to management

The fifth function of QA personnel is to report to management. Regular reports on compliance with *general* standards and *specific* standards must be prepared. Reports must be positive in nature, contain no surprises, and be based on sound analyses that are supported by concrete facts.

6. Training in QA standards and procedures

The sixth function of QA personnel is to train all other information systems personnel in quality assurance standards and procedures. One type of training focuses on *general knowledge* about standards and procedures. Another type focuses on *specific training* that is needed to support the development, implementation, operation, and maintenance of a specific application system.

ORGANIZATIONAL CONSIDERATIONS

1. Placement of QA function

QA function should be placed in the organizational hierarchy of the IS function so that it can operate independently of other IS activities. The manger of the QA function should report directly to the executive who is in charge of the IS function. QA personnel should be afforded sufficient status so they can operate effectively.

To operate effectively, QA function must also have proper approved charter. The charter should lay out clearly the rights and responsibilities of the QA function. Job positions must also be defined and authority and accountability should be specified.

2. Staffing the QA function

Properly staffing the QA function can be difficult to accomplish. QA personnel need to be well trained and competent and their skills must be up to date. They must also have a high level of interpersonal skills. Many information systems personnel prefer to engage in development work rather than quality assurance work. Consequently, management must sometimes work hard to attract high-quality staff into QA function.

RELATIONSHIP BETWEEN QUALITY ASSURANCE AND AUDITING

In many ways, the objective of and functions of QA personnel and auditors are the same. Both also are concerned with ensuring high-quality information systems are developed, implemented, operated and maintained. Both also are concerned with collecting evidence on and evaluating the reliability of IS controls. As a result, the auditors often can place greater reliance on controls and reduce the extent of substantive testing work when a QA function is in place and working reliably.

Performance Measurement Tools

Performance measurement tools enable auditors to obtain evidence on factors relating to system efficiency.

For systems that are already operational, auditors can use them to diagnose problems and construct tuning therapies.

Auditors can also use them to estimate the parameter values required in analytical and simulation performance evaluation models of computer system.

All characteristics that auditors might measure in computer systems fall into ***three*** classes:

1. **Performance indices**, which auditors used to assess whether a computer system is performing satisfactorily
2. **Worked load parameters**, which auditors used to characterize the resource demand that will be placed upon a system
3. **System parameter**, which auditors used to characterize those factors that effect the system capability to deal with the work load demands placed on it.

Performance measurements tool have ***five*** basic ***components***:

1. **Sensor or probes**, which detect the occurrence or non occurrence of events and the magnitude of events
2. **Selector**, which designate the subset of event to be monitored from the set of all event that the tool can detect
3. **Processors**, which transform the data collected into a form suitable for storage and output
4. **Recorders**, which write the data collected to a permanent storage medium ;and
5. **Reporters**, which summarize the information stored and present it to the users.

Performance measurement tools can undertake ***five*** types of ***measurements of resource consumption*** events:

1. **Trace**, which is recorded sequence of occurrence of events.
2. **Event duration**, which is real time consumed by an event.
3. **Relative duration**, which is the ratio of the total real time consumed by an event to the total elapsed time.
4. **Event frequency**, which is the number of time s and event occurs over a give time period ; and
5. **Distribution of event,** which is the distribution of event times over some elapsed time period.

Overall capabilities of a performance measurements tool are a function of ***seven*** attributes of the tool:

1. **Artifact** - which is the extent to which the tool causes overheads and interferes with the normal operation of the system
2. **Domain** - which is the number of different classes of events that the tool can detect
3. **Resolution** - which is the maximum frequency with which the tool can detect events and record them correctly
4. **Input width** - which is the number of bits of input data the tools can extract and process when and event occurs
5. **Data reduction capabilities** - which indicate the extent to which the tool can summarize data before it is stored.
6. **Data storage capabilities** - which indicate the amount of permanent storage available for recording data: and
7. **Precision** - which is the number of digits available to represent data

Performance measurements tools can be ***classified*** in a number of ways.

a) Event-driven tools are triggered by the occurrence of an event. They are useful when the frequency with which an instant of an event type occurs is low.

b) Sampling tools are activated by some type of timing mechanism.

c) Online tools display their results continuously or after short period of time have elapsed.

d) Batch tools store their performance measurement data for presentation at a later time.

TYPES OF PERFORMANCE MEASUREMENT TOOLS

A) HARDWARE MONITOR
A hardware monitor is a device connected via probes to a target computer that detects signals in the target computer electronic circuitry. It causes minimal or no interference in the target system. It is also able to detect very short duration events in the target system. It can not trace software-related events, however

B) SOFTWARE MONITOR
A software monitor is a program subroutine or instruction inserted into the code of a system or another program to collect performance measurement data. It can measure the occurrence of more macroscopic events then hardware monitor, such as a program assess to a record in a data base. It major limitation is that it introduces artifact into the target system.

C) FIRMWARE MONITOR
Firmware monitors used microcode in the target system to measure events. Because the execution time for a micro instruction is shorter than a normal program instruction. Firmware monitor produce less artifact than software monitor. Moreover, they can access some hardware indicators that cannot be access by software. Thus, their domain over lapse both hardware monitors and software monitors. Microcode has a constraint space, however, and thus only a limited number of probes can be inserted for monitoring purpose.

D) HYBIRD MONITOR
A hybrid monitor has hardware, software and perhaps firmware components. These components can be configured in many different ways. For example, software and firmware probes can detect events and write them to a hardware interface. An external device that reads processes stores and present the data written to the hardware interface. Thus, hybrid monitor can detect both software and hardware related events. They are sometimes difficult to use. However, because of the measurement taken by the software component the measurement taken by hardware component must be coordinated.

Performance measurement data can be presented by either using tables or charts. ***Two*** types of charts that are often used to present performance measurement data are:

Gantt charts: Gantt charts use the horizontal bar to show the percentage utilization of a resource and the extent of overlap of resource utilization among a number of resources.

Kiviat graphs: Kiviat graphs presents performance measurements results so the problem with the performance can be recognized easily. They use radial axes in a circle to plot performance measurement results. The shape of the resulting plot can be used to determine the extent to which the system is balanced in terms of its resource utilization.

Auditors should have ***two*** concerns about data integrity whenever performance monitors are used

First, they should determine whether the monitor has been installed correctly in the target system. They must evaluate the integrity of the measurements made by the monitor and the integrity of the target system processes after instrumentation.

Second, auditors must try to determine whether a monitor has been used to violate data integrity. They should evaluate whether unauthorized use of the monitor to breach data privacy.