SYSTEMS ADMINISTRATION, CONTROLS AND AUDIT

Systems Administration

- System administration covers a broad area of hardware and software setup/installation, configuration, administration and maintenance.
- It involves the setup of systems mostly in a network which covers: user administration, resource management, configuration management, performance management and maintenance.
- In practice it falls into the two main areas of network administration and database administration.

Responsibilities of Administrators

- Creating and managing user account
- Training and supporting users’ needs
- Enforcing security standards
- Tuning the network and database for maximum performance
- Troubleshooting the system
- Monitoring and regulation the server storage space
- Adding users and systems to the network

Network Workgroups and Domains

a. Workgroups

- Computers in workgroups are organized according to department.
- Microsoft **My Network places** provides a list all computers in the workgroup that have sharing enabled.
- Browse the E**ntire Network** to see the list of workgroups on the network.
- Each workgroup is browsable
- Any computer can join a workgroup by simply specifying the workgroup name.
- Workgroups require that each user manages his own resources and users. (user- level security). (Windows 95, Windows for workgroup, NT servers / workstations, Windows 98, 2000pro and XP are capable of joining the workgroup)

b. Domains (Server -based) networks

- Sever-based networks offer higher security and central administration. There are two types of domain

- Primary Domain Controler (PDC) (Validates users accounts at login)

- Backup Domain Controller (BDC) (Assists with logins if PDC is unavailable)

- Each user must have an account before he can logon.
- Upon logon to the Domain, resources are granted based on the rights and privileges assigned the account.
- Domain provides central administration and accounts for the network.
- Domain provides central database of users and groups which are granted rights to resources throughout the domain.
- (Windows 95, Windows 4 workgroup, NT servers/workstations, Windows 2000 Server and 2003 are capable of joining a domain.)

Creating User Accounts

Users

- For anyone to access resources on the network, a user account must be created. A user account identifies the user on the network, and allows right to be assigned. User accounts can be created on each computer or the entire domain.
- Maintenance of accounts on domains are easier because of centralized system and the Administrative Tools program on the operating system is needed to manage user accounts. Other features include:
- Security Identifier (SID), is a number that identifies an account. SIDs are very large numbers that are unique in the universe.
- All rights assigned a user are identified with the account number. When a user account is deleted the number is lost and when another is created even with same name, a new number is assigned.

Creating User Account Cont.

Rules for creating accounts

- A user account can be up to 20 characters using a combination of letters, numbers and symbols.
- Special symbols: /, \ , ; , : , !, = , + , <, > , etc. are not permitted.
- Standard information needed include:
- **User name** -the name used to logon to the network. A short name that identifies the user
- **Password** -a secret word that provides security for the user account.
- **Full name** -the full names of users is needed for information purposes.
- **Description** -this refers to the role of the user in the company.
- **Home directory** -the personal directory on the server where the user saves his work.
- **Login scripts** -the scripts set up the network environment for the users, it is executed upon logon.

Creating User Account Cont.

Password

- This is a secret word through which a user gains access to a network or resources. The network is only as secured as the user's password. Some rules are that:

- It should not be obvious like your name, your car name and birthday.
- It should be memorizable, do not write it down.
- It should be changed often.

Special accounts

1. Administrator Account
2. Guest Account
3. Group Account

Creating User Account Cont.

Types of Group

a. **Local groups** -These are created and stored on each local computer security database. They are used to group users on a single server or domain.

b. **Global groups** -These enable you to share group information between domains and servers. They are used across the entire domain.

c. **Special groups** -This group is used by NT to handle users dynamically. The administrator cannot control the membership of this group. NT does it automatically.

Creating User Account Cont.

- Examples are Interactive and Network groups. The interactive group is composed of users who are physically working on the computer console. The Network group is composed of users who use the computer resources across the network.

d. **Built-in groups** -These are groups are automatically created during installation. They include:

- **Administrator** -It includes network administrator with full rights to the server-
- **Operator-type group** -It grants members access to system function (backup and restore)
- **System groups**- It is used to manage data.

SECURITY METHODS

- Data is the raw material upon which information is produced. Thus, it is the live-wire of all organizations. Therefore, disaster recovery plans must be put in place to safeguard its corruption and loss.
- There are two types of security on a network. This type depends on the network and the operating system. The two types are:

(a) Share-level security

- Share-level security relies only on a single password to access a resource. It is used in workgroups.

(b) User-level security

- This requires a user name and password to logon to the resources. It is used in domains.

SECURITY METHODS Cont.

Auditing

- Auditing helps to track events on the network. The events tracked include:
- Users loggin and logout,
- Access to files and directions,
- System reboot.

Audit logs help administrators to track unauthorized access, and common mistake on the part of the administrators. Common events audited include:

- Login successes and failures attempts
- Connections to network resources, printers and drives
- System reboots
- Password changes
- Opening and closing of files -Permission rights changes
- User/group accounts created/deleted

FAULT-TOLERANCE METHODS

- The available fault-tolerance methods include:

1. Data backups
2. Data redundants
3. Uninterruptible power supply.

1. Backups

- Backup is one of the very common and prominent ways of safeguarding data. Most enterprises carry out data backup on a regular basis. Thus, data storage on disks, tape and W/R CDs are used to backup and archive data.

Fault-tolerance Methods Cont.

- There are a number of methods employed in backing up data. However, the method used depends largely on the amount of data, and the length of time needed to do the backup and restore it. These methods include:
- **Full backup**: It backs up all selected files. This process marks the files as archived.
- **Incremental backup:** It backups selected files that have been changed since last backup. The files are thus marked as archived.
- **Differential backup**: It backs-up files that have changed since last backup. The files are not marked archived.
- **Copy backup**: It backs-up selected files without marking them archived.
- **Daily backup:** It backs-up selected files that have changed during the day without marking them archived.

Fault-tolerance Methods Cont.

2. REDUNDANT SYSTEMS

- This is another fault-tolerant system that is used in conjunction with backups. The method involves duplicating data across several drives or different partitions. It is not a replacement for backups.
- Redundant Arrays of Inexpensive Disks (RAIDs), offers several levels of fault tolerance. RAIDs use a combination of hard drives to provide a high level of fault tolerance or to provide greater speed when accessing data on the drive. The common levels of RAIDs are 0, 1, 2, 3, 4 and 5. RAID 2, 3 and 4 are not normally used because of their limitations. Microsoft chose RAID 5 because it evolved from 2, 3, and 4.

Fault-tolerance Methods Cont.

3. UNINTERRUPTIBLE POWER SUPPLIES (UPS)

- UPS is used to safeguard against power outages. It is a battery that operates between the power outlet and the computer.
- The size of the battery varies but it is important having one that is powerful enough to sustain the equipment.
- UPS sends valuable information such as power conditions and the battery life to the computer. Whenever there is power failure, it alerts the user so that he can save his jobs and shutdown the system in an orderly manner to avoid corrupting the data.
- There are some OSs that have the capability of communicating with the UPS.

Fault-tolerance Methods Cont.

PERFORMANCE

- Performance monitoring helps to monitor performance of systems and the network. That is, the monitoring of memory usage, CPU utilization, the available disk space, and bandwidth utilization.
- Performance monitoring helps reveal systems faults: cables, connectors, overloaded segments, and failed segments.
- Some server OSs, include the facilities to monitor performance. Similarly, a third- part software such as Simple Network Mail Protocol (SNMP) offers many statistical information concerning performance monitoring.

CONTROL SYSTEMS

- Controls are built into systems to forestall the occurrence of unforeseen circumstances that may be detrimental to the overall goal of the system.
- Some controls have the capability of sensing and predicting the state of the system by comparing the various states with the benchmark and initiates corrective measures if the situation is abnormal.
- Examples of these control systems are feedback and feedforward controls. Some controls on the other hand have the capability of preventing the occurrence of this abnormal situation, such controls are called preventive controls.
- The three control systems are mostly used in manual information systems. Therefore, it is the responsibility of management to consider the cost-benefit dimension of instituting a control system.

Control Systems Cont.

1. Feedback Control Systems

- A typical feedback control system is composed of two main modules, namely:
- **Process** – This is responsible for accepting inputs and converting them to outputs. A Sensor is contained within the process and is responsible for monitoring the state of the process.
- **Controller** – This component is responsible for collecting data from the sensor, comparing it with the benchmark and generates feedbacks that are used to effect the process. The controller contains two elements: effector and comparator. The comparator is responsible for comparing the sensed data with the benchmark to generate a signal to the effector, which in turn, makes adjustments to the output based on the generated signal.

2. Feedforward Control Systems

- The Feedforward control system is similar to the feedback control system in a number of respects. The fundamental difference between the two is that while the controller in feedback control system compares the sensed data with the benchmark in order to make adjustments to the system, the controller in the feedforward system uses the sensed data to predict the future state of the system, which is then compared with the future standard set.
- Consequently, the controller in the feedforward control system is composed of an additional element called the predictor that takes a sensed data, apply a suitable predictive model to estimate the future state of the system. Subsequently, the prediction is fed into the comparator and effector so that the necessary adjustments are put in place to ascertain that future objectives are met. Generally, the feedback control systems are reactive while the feedforward control systems are proactive.

Control System Cont.

3. Preventive Control System

- Preventive controls constitute an integral part of both manual and computerized information systems. They are primarily instituted to prevent undesired events from occurring.
- Unlike both feedbackward and feedforward controls that work through a controller that is resident outside the process, preventive controls reside mainly within the process.
- Therefore, preventive controls are categorized into:

a. Documentation

- Provision of appropriate documentation will help a great deal in minimizing unintentional errors in recording, inputting and processing.

Control Systems Cont.

b. Procedures Manual

- Procedures manuals help a great deal to prevent inconsistencies that may arise from transaction processing and the general operations within the organization. The manual is expected to contain in specific terms, the job specifications of each staff of the organization, and it helps to identify the sources of whatever errors that may arise in the course of the company's operations.

c. Personnel Control

- It is the responsibility of the human resource manager to hire the appropriate workforce needed to deliver the goals and objectives of the firm.
- Consequently, it is expedient that the appropriate personnel must be selected, trained and retrained to deliver on his job specifications.

Control Systems Cont.

d. Physical Controls

- A prominent way of preventing illegal loss of assets and cash is to offer restricted access to offices where such valuables are kept. The available physical control include: access-locks, safes, fences, solid and well fortified walls and doors.
- In addition to the restricted access to staff, physical control should also guide against a range of natural hazards that may befall the entire system. Thus, fire extinguishers, lightning arrestor, etc must be visibly present.

Control Systems Cont.

Controls of Computerized Information Systems

- **Goals of Control**
- The primary aim of instituting controls in any system is to offer:

i. Deterrence and prevention: Deterrence of potential frauds and prevention of erroneous data.

ii. Detection: Detection of erroneous or accidental error of fraud and corrective measures put in place for correction.

iii. Loss Minimization: Controls are put in place to reduce the magnitude of loss, financial or otherwise that may occur accidentally by providing backups of transactions.

Control Systems Cont.

iv. Recovery: In case of disaster or accidental loss of data, a recovery plan should be such that will help recover the lost data with minimum effort.

v. Investigation: It is common practice nowadays to create an internal audit unit within a firm to monitor and control the firm’s transactions on a daily basis, while an external audit unit is external to the firm and brought in usually once in a year.

- Generally, controls within a computer system are instituted across the input, storage, processing, output and data transmission levels.

1. Input Controls

- Input Controls are instituted around the following issues such as accuracy, completeness and recording which are considered in reducing the amount of errors that goes into the system.

Control Systems Cont.

a. Accuracy Controls

- These controls involve:

i. Format checks: This is a check to ascertain that input data is fed in according to the prescribed format.

- e.g. MM/DD/YY for date or XX-YY-9999 for matriculation number, etc.

ii. Limit Checks: This check is used to ascertain that the supplied data is within a specified range, that is a specified lower and up bounds. E.g. [200-300] or [2005-2007], etc.

iii. Reasonableness checks: This check is used to verify the given data by comparing it with the previous one in case of any discrepancies and the justifications for such if it must be used.

Control Systems Cont.

iv. Check-digit verification: This is used when entries are expected to be made under some specified coded headings. Such coded headings or digits are prone to transcription errors which can be of great consequences to the system e.g., An account code: CU940017 and CU49017.

v. Master-file checks: This check is used whenever the master-file is to be updated with the transaction file in an online processing system. Both the transaction file and the master file are indexed according to a specified field for effective match.

Control Systems Cont.

b. Completeness totals

- Incompleteness errors involve incomplete entry of data. The available controls include:

i. Batch control totals: Transactions can be grouped together in batches of invoices or order. The total of each batch, which is the sum of all the transactions in that batch is calculated manually and used to compare with the computer generated total. The control total can be used to ascertain that the complete transactions have been considered.

ii. Batch hash totals: Hash total is similar to control totals. A hash total may be the sum of all the customers' identification numbers in a particular batch, which may be meaningless but can be used to test for completeness by comparing it with the computer generated hash total.

Control System Cont.

iii. Batch record totals: This involves keeping a count of the various records in a particular transaction which is used to compare with the computer generated count after processing to ascertain that all the records was treated.

iv. Sequence Checks: This involves pre-numbering all the documents for processing before entry, while the computer is made to perform a sequence check and print any missing number detected.

v. Field-filling checks: In online transactions, some fields are very critical that values must be entered before any processing can be done. This is very common in web transactions and failure to enter any value, the system prompts the attention of the user to it.

Control System Cont.

c. Recording Controls

- These controls are used to provide a detailed documentation of all the transactions that are carried out in the system. They include:

i. Error log: During transaction processing, any erroneous transaction is written to the error long, which is investigated at the end of processing for correction and rerun. Error log is usually system generated.

ii. Transaction Log: This provides a detailed record of all transactions that are processed by the system. This record include: reference number, date, type of transaction, account number, input day, etc. transaction logs are generally used for audit trail as they contain details of transactions that can be consulted for possible fraud.

Control System Cont.

d. Storage Controls

- Data is one of the most valuable assets of any organization and concerted efforts must be made to safeguard the integrity of the database. In addition, effective controls must be instituted against accidental erasure, fire and natural hazards, as well as putting in place an efficient backup and recovery plans. Such controls include:

i. Physical protection against erasure:

ii. External labels:

iii. Magnetic labels:

iv. File backup routines:

v. Database concurrency controls:

Control System Cont.

e. Processing Controls

- The processing controls include:

i. Run-to-run controls: A particular computer operation may involve the processing of several separate but related transaction processing. Each of such processing is called a run and the control totals implemented by each run can be passed from one to another for completeness check. This is run-to-run control.

ii. Hardware controls: These are controls that are designed to offer fault detection, avoidance and tolerance. These are provided through disk duplexing, disk mirroring, redundant array of independent disks (RAIDs) and disk backup. Some controls are circuitry based such as run-time errors, data overflow and lost sign.

Control System Cont.

f. Output Controls

- These controls are aimed at ascertaining the correctness and completeness of the generated results as well as the correct dissemination of the results to the authorized recipient. They include:

i. Control totals: This is a control instituted to detect data loss or addition.

ii. Pre-numbering: All the output documents should be pre-numbered and accounted for.

iii. Authorization: Some staff is given authorization to handle some documents. Such outputs must be taken to them in a secure manner.

iv. Sensitive output: Confidential outputs are directed to an appropriate quarters in a safe and secure manner to prevent unauthorized staff from gaining access to them.

Control System Cont.

g. Data Transmission

- The advent of the Internet, extranet and intranet has offered an efficient means of disseminating information around the world or within the office.
- These technologies involve the use of telecommunications devices and the computer systems to transmit information from one place to another. All communications are subject to a number of errors which are guided against by:

i. Parity Bit Control

ii. Echo Checks

iii. Control Total

iv. Integrity checks