ASPECTS OF BUSINESS AND CONTROL CONSIDERATIONS IN COMPUTER NETWORK SYSTEMS

by

JOHANNES JACOBUS ROSSOUW

ESSAY

submitted in part fulfilment of the requirements

for the degree

Master of Commerce

in

Accounting

in the

Faculty of Economic and Business Sciences

at

Die Randse Afrikaanse Universiteit

Study leader: Prof F Nel.

JOHANNESBURG.

NOVEMBER 1989.

DECLARATION

I declare that this research essay is my own unaided work. It has been submitted in part fulfilment of the requirements of the degree of Master of Commerce at Die Randse Afrikaanse Universiteit, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Johannes Jacobus Rossouw

30 November 1989

TABLE OF CONTENTS

CHAPTER 1 - PURPOSE AND METHOD OF STUDY

1. Purpose of study

During one of the initial stages of preparation for this degree, the more important issues of Generalised Message Control System (GEMCOS), a message control system used in a Burroughs mainframe environment, were studied and identified from an auditing point of view. This study resulted in the need to study computer networks in more detail. Certain aspects of computer networks were identified for the purpose of this study. That purpose is as follows:

- to define a computer network;
- to study briefly the history of computer networks;
- to identify the main computer network configurations (topologies);
- to identify aspects of some of the more important communicating principles;
- to briefly refer to some important business considerations; and
- to identify the more important controls in a computer network system.

As financial institutions are the major users of computer networks in South Africa, some reference is made to financial and banking institutions.

2. Method of study

The study takes the form of a literature study.

CHAPTER 2 - COMPUTER NETWORKS: INTRODUCTION AND HISTORICAL OVERVIEW.

1. Introduction

A number of definitions exist for defining a computer network:

> "...a computer network can be defined as a single computer, called a 'host', together with communications circuits, communications equipment, and terminals... A computer network can also be defined as two or more computers connected via a communications medium, together with associated communications links, terminals, and communications equipment..." (Stamper 1986:25);

> "...a number of devices (computers, terminals, etc.) interconnected in some way with each device capable of autonomous processing" (Bacon et al., 1984:49);

> "...a set of autonomous computer systems, interconnected so as to permit interactive resource sharing between any pair of systems" (Bacon et al., 1984:49).

From the above definitions it is evident that communication forms a vital part of a computer network. However, the terms "communication" and "interconnection" are not defined and no distinction is made between "data communications" and "computer communications".

Chou (1983:1) has identified three different interpretations of the term "computer communications" :

"Interpretation 1
An interconnected group of independent computer systems which communicate with one another and share resources, such as programs, data, hardware, or software;"

"Interpretation 2
An interconnected group of independent computers and data terminals which communicate with one another;"

"Interpretation 3
Any data communication network which consists of at least one computer system."

Interpretation 1 excludes computers "...used solely for handling communications or controlling terminals..." (Chou 1983:1). Interpretation 2 includes "...computers used for handling communications or controlling terminals, such as concentrators and terminal control units..." (Chou 1983:1). Interpretation 3 virtually does not distinguish between data communication and computer communication (Chou 1983:1).

Chou (1983:2) distinguishes between "data communication" and "computer communication" in that no computer-to-computer communication is involved with "data communication", and computer-to-computer communication exists in "computer communication".

Stamper (1986:2) distinguishes between "telecommunications" and "data communications". Telecommunications include "any process

that permits the passage from a sender to one or more receivers of information of any nature delivered in any usable form ... by means of any electromagnetic system..." He defines data communications as "that part of telecommunications that relates to computer systems, or the electronic transmission of computer data." However, this definition excludes the transmission of data to local peripherals such as disk, tape and printers.

As this study investigates aspects of business and control considerations computer network systems, a computer network is defined as follows :

> A computer network comprises two or more computer systems and other devices interconnected via a communications medium and communications equipment permitting resource sharing and autonomous processing.

2. Historical overview

The first experiments which involved computer networking in its simplest form was the interconnection of two computers, the TX-2 at the Lincoln Laboratory with the Q-32 at System Development Corporation in the USA. The early problem was the protocol for the connection and the problem was overcome by treating the computers as extensions of the monitors for each system. This made it possible not only to transmit data but to include error correcting and recovery capabilities (Bacon et al., 1984:52).

Another early network was that of APRANET, interconnecting a

a number of defence research sites in the USA on an experimental basis. APRANET was the first major network and achieved the following goals :

- at least two communication paths existed between every node;
- an undetected error rate of one bit in a million million;
- less than one node failure per day; and
- a maximum transmission time between nodes of 0,5 seconds.

A major design characteristic was to separate the "host" computer from the communications sub-network so that, in the event of a host failure, the fault was isolated from the network, provided that the host/sub-network connection could prevent the error propagating in the network. During the mid-1970's the Defence Communication Agency took over APRANET as a functioning network (Bacon et al., 1984:53).

Other early networks included the General Electric Mark III system and Timeshare Incorporated's TYMNET. The GE Mark III system was different to that of APRANET, as it provided a terminal-to-computer connection rather than a computer-to-computer connection. The system had a hierarchical configuration, as users accessed remote concentrators which were linked to central concentrators, which were themselves linked to the computer centres. Terminal access and remote job entry access were available on this system. TYMNET had the facility that, although the network was supervised by a single computer, in the event of its failure, its functions could be taken over by another, and so on. This capability provided a high degree of network integrity (Bacon et al., 1984:53).

CHAPTER 3 - NETWORK CONFIGURATIONS AND COMMUNICATING PRINCIPLES.

1. Network configurations

There are many topologies available that may be used for computer networks, but there are significant implications for the network designer. There are two major topologies for networks, the star network (fig. 1) and the ring network (fig. 2) (Bacon et al., 1984:57,58).

Figure 1: Star network

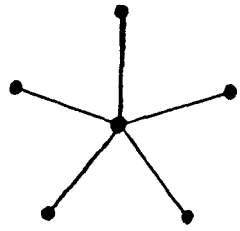
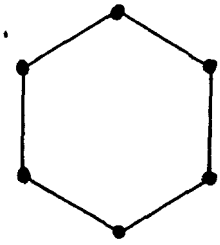


Figure 2: Ring network



Other topologies include the hybrid topology (fig. 3) (Watne & Turney 1984:476), and the bus topology (fig. 4) (Page & Hooper 1987:184,185). The hybrid network contains elements of star and ring configurations. Several computers can be connected in a ring configuration, whereas each computer could be the centre of its own star configuration. The bus or tree configuration is a connection of several computers to a common core wire.

Figure 3: Hybrid network

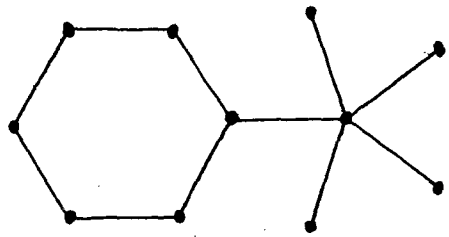
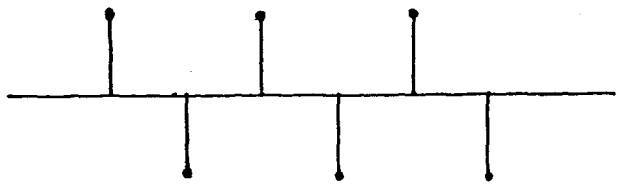


Figure 4: Bus network



Variations on the above networks include the fully interconnected network (fig. 5) (Bacon et al., 1984:58; Watne & Turney 1984:477), the hierarchical network (fig. 6) (Bacon et al. 1984:58), and the ring-switching network (fig. 7) (Chou 1983:5).

Figure 5: Fully interconnected network

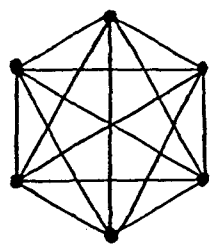


Figure 6: Hierarchical network

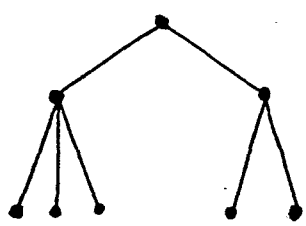
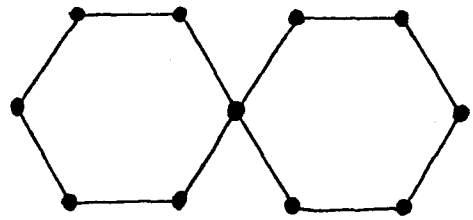


Figure 7: Ring-switching network



2. Communication principles

Message transmission can be achieved by direct connection, relaying, switching, or a combination of these.

Direct connection

In a direct connection architecture, individual units of data terminal equipment (DTEs) communicate with each other directly through a common channel. When one DTE transmits a message, all other DTEs that share the same channel receive the message at about the same time. Since more than one DTE might attempt to use the common channel simultaneously, a control procedure must handle any contention problems. Procedures for controlling multiple accesses to the common channel are called multiple-access procedures. Multiple accesses are achieved by static or dynamic allocation of the channel. Static allocation of the channel involves the division of the channel into sub-channels, with each DTE having a dedicated subchannel. Every DTE has a dedicated channel for transmission but may receive information from the whole channel. Multiple accesses can also be achieved by the dynamic allocation of the channel, based on the capacity and time duration of assignments. The capacity and time duration of assignments are dynamically determined to meet the changing demands of DTEs. A set of built-in rules schedules the traffic to

optimise channel utilisation and minimise conflicts. Optimising of channel utilisation is achieved by three techniques, the polling technique, the random-access technique, and the reservation technique.

The polling technique involves a specific DTE being designated as the primary station and all other DTEs secondary stations. The primary station polls the secondary stations one by one to enquire whether there are messages to be sent. After a secondary station has responded, either negatively or positively, the next secondary station is polled.

The random-access technique involves the DTEs seeking access to the same channel via interface devices. In the slotted random-access scheme, time is divided into slots and a DTE can only access the channel at the beginning of a time slot. The random-access method is well suited for systems where the time interval needed for each transmission is very short relative to the interval between transmissions.

The reservation technique requires DTEs to make reservations for one or more slots before initiating transmission. DTEs make reservations to a specific central or control station. The central station dynamically assigns the channels to the requesting DTEs. The reservation technique is well suited for systems where there are a small number of stations with a large volume of transactions (Chou 1983:2-4).

Shifting or Relaying

In a ring network a DTE must connect to a ring interface processor (RIP) in order to communicate with other DTEs in the network. Each RIP is connected to the ring through a shift register bridging its input and output lines. The traffic circulates the ring as a continuous bit stream from one RIP to the next. If an input to RIP is not addressed to one of its local DTEs, it is relayed to the output through the shift register without storing the input at the RIP. In the synchronous transmission mode, the band-width of the network is divided into time slots. Each slot is specifically dedicated to transmit messages originating from a particular RIP. In the asynchronus transmission mode there are no fixed time slots or message sizes. Messages generated from different RIPs may overwrite each other if they are allowed to be forwarded onto the ring network simultaneously. A method of avoiding overwriting is to have a "token" circulating around the ring. A RIP grabs the token before it transmits and releases the token after the transmission. While the token is RIP resident, input messages cannot be forwarded to the output and overwriting is thus avoided. RIP access to the ring network can be controlled centrally by one or a small number of processors, or it can be controlled on a distributed basis where control is distributed to most, if not all, of the processors. Two or more ring networks can be interconnected via RIPs that switch the messages from one ring to another (Chou 1983:5-7).

Switching

In a switching configuration, communicating stations do not have to be directly connected. Transmission of a message from one station to another can be made via intermediate stations.

Intermediate stations, also referred to as switches, put input messages on output links which are determined by the network routing strategy. Switches are either circuit or store-and-forward switches. Store-and-forward switches are generally known as packet or message switches.

In a packet or message switching network, the message is completely received and stored in memory at each of the switches. Based on a routing table in the switch, the message is then routed to the next switch on the route. In a packet switching network, any message longer than a specified size is subdivided into specific-sized packets before transmission. Messages are reassembled at the recieving end. Packets can be stored in the main memory of the switches. The segment sizes of a message-switching network are as long as the longest message. Message-switching systems use predetermined paths and store messages in secondary memory instead of main memory. However, a detailed journal is kept of each message.

In a circuit switching network, the whole path must be available and allocated between the source and destination DTEs before the message can be transmitted. This approach uses more set-up time as every line on the path must be available before a transmission can start. It also uses more network resources, as the whole path must be reserved before transmission commences. However, circuit switching has distinct advantages. Communication control overhead traffic is less. With packet switching, the overhead from control traffic can be substantial. Circuit switching is well suited for continuous or large streams of traffic. Other advantages are that

there is no code, format, speed, or protocol conversion, and no intermediate device can intercept or alter the content of messages between end users (Chou 1983:7-12).

3. Other technical aspects

Four fundamental technical problems in network design have been identified by Frank (1972:167):

1. Where lines should be put in the network;
2. What the capacity of a line should be;
3. The relative importance of reliability;
4. What traffic load is to be sustained.

In the optimal network design, minimisation of time delay and costs is of utmost importance. The factors to be considered in determining the minimum time delay and cost are:

- size of node buffers;
- line speeds;
- types of lines;
- prices of lines;
- traffic load;
- routing; and
- number of lines between nodes (Frank 1972:180).

Frank (1972:182) also states that network routing and configuration must be solid enough to handle wide variations in traffic. Beauchamp (1987:94) states that control for data flowing through a switched network is vested in the nodes. He identifies three areas of control which is carried out at node level, namely:

routing;

flow control; and

error control.

Routing

One method to control routing is to make use of routing tables situated at specific nodes. This method is known as deterministic or fixed routing (Beauchamp 1987:95). Adaptive routing, where use is made of dynamic information on the current traffic flow which is applied to modify the fixed tables, is more useful than the deterministic routing option. Adaptive routing is, however, only partially effective as it is difficult to obtain routing information available at distant nodes in remote parts of the network (Beauchamp 1987:96). Three types of adaptive routing methods can be applied:

- isolated adaptive routing makes use of information available locally in each node;
- distributed adaptive routing has the object of finding the path of least delay for the network traffic. Average delay is measured at each node and information is propagated to other nodes in the system. Each node can use this information in computing the fastest path to ongoing nodes;
- flooding and random routing dispense with a formal systematic routing algorithm. Multiple copies of the packet are forwarded to all onward nodes in the case of flooding. The number of nodes to be traversed to reach the destination is calculated (also known as the hop count), and the packet following the shortest route is preserved. The other packets are destroyed. Neither of these methods requires information about the network topology (Beachamp 1987:96-98). When using random routing, a

random choice of an output path is made at every onward node. The hop count is used in deciding upon the elimination of a packet at a given node.

Flow control

"Flow control means the methods used to keep network data moving" Beauchamp (1987:98).

"Flow control methods are generally based on the acknowledgement of packets transmitted by the source and received at their destination" Beauchamp (1987:98).

Flow control should ensure that receiving nodes do not accept packets at a rate greater than the end device can accept them. Flow control should also ensure that the network does not become congested with packets and that the total number of packets in transit does not exceed the total storage capacity of the network. With the stop-and-wait flow control method, packets are sent one at a time between nodes, and are acknowledged with a signal when successfully received. If the acknowledgement signal is not received before the expiry of a predetermined time interval, retransmission of the last packet sent is done. With the sliding window method, multiple packets rather than a single packet may be in transit at a given time. The order of reception, however, is important so as to ensure that the packet has been received completely and accurately. Acknowledgement of receipt and time-out are also used with this method.

3. Conclusion

The network configuration decision depends upon the information and processing requirements at the geographically dispersed locations. Users could be grouped geographically. The communication technique depends upon the network configuration, strategic communication requirements, transmission times, controls required, and physical and hardware constraints.

CHAPTER 4 - BUSINESS CONSIDERATIONS

Weis (1972:1) identifies three types of business networks:

Remote Job Entry networks;

Batch and Interactive Networks; and

Resource-Sharing Networks,

and states that the problems in a network environment become more interesting and difficult to solve as the functional capabilities of the network increase. Weis (1972:2) classifies these three types of networks in definite classes in terms of their functional capabilities. The Remote Job Entry network has basic capabilities and the full Resource-Sharing Network has advanced capabilities. Weis (1972:12-22) identifies the following major problems in networks:

architectural philosophy;

resource control;

data interchange;

telecommunications; and

technical management.

These aspects are now discussed briefly.

Architectural philosophy

Two architectural philosophies are identified:

Centralised networks; and

Distributed networks (Weis 1972:13).

In a centralised network, central control facilities exist and this approach tries to minimise resources. However, individual users cannot operate independently of the central facility. In a

In a decentralised network, network functions are more evenly allocated to all nodes within the network (Weis 1972:13). The architectural philosophy chosen will therefore determine the resource control problems and the cost of resources and resource control.

Resource control

If an installation is incorporated into a network, the installation manager, or higher authority, will decide which processing capabilities will be made available to the network and which processing capabilities of the network will be made available to the installation. Weis (1972:15) identifies security as the immediate problem in a network. He also justly states that security problems are greatly magnified in a network environment. Weis (1972:16) also identifies the problem of users at a particular installation becoming dependent upon facilities offered by other installations within the network over which the user has no control. Projects becoming dependent on external resources may be crippled.

Data interchange

Weis (1972:18-19) identifies the following data interchange problems that should be addressed within a network:

- transporting of data between systems;
- different operating systems;
- source language incompatibility; and
- different CPUs.

System designers have problems with data communication due to the large number of manufacturers of data communication equipment and the lack of standards that permit easy integration of units. Due to the above, problems may be encountered when hardware and software from

different suppliers are to be integrated (McLeod 1983:301-302). The major computer manufacturers, however, have introduced standards. Examples are:

IBM	- Systems Network Architecture (SNA);
Sperry Univac	- Distributed Communications Architecture (DCA);
NCR	- Distributed Network Architecture (DNA);
Burroughs	- Burroughs Network Architecture (BNA).

Network architectures are generally characterised by levels of physical network connections and layers of logical network connections (McLeod 1983:302). Lorin (1980:92) and Beauchamp (1987:169) also emphasize the existence of different layers, and describe the ISO X.25 seven-layer communication model. The International Standards Organisation (ISO) introduced the X.25 international protocol standard for transmitting data from one node to another during 1976 (McLeod 1983:304). Beauchamp (1987:179) states that the X.25 protocol can be used in local area networks, but is more suitable for wide area networks.

It is obvious that the impact of different standards, technology and therefore layering, should be borne in mind from a business and control perspective.

Telecommunications

Communication standards, not necessarily identical throughout the network, that provide the maximum flexibility, are the most desirable in a computer network (Weis 1972:20). In addition to flexibility, the next important problem identified is the placing of the

telecommunication functions, especially functions such as compaction and cryptography (Weis 1972:20). In the banking environment cryptography becomes very important, especially in foreign exchange systems.

Technical Management

Weis (1972:21) identifies the problem of maintaining control over modifications in operating systems. He suggests that a central library facility for system source maintenance will alleviate part of the problem. Another area of difficulty is network accounting. McKay & Karp and Lorin have also identified certain important business aspects that should be borne in mind. These aspects are now referred to briefly.

McKay & Karp (1972:29) have identified services that a network must be able to provide. These are as follows:

- users should be provided with easy access and use of programs and data throughout the network;
- extensive use of existing communication and hardware facilities should be provided;
- interaction of heterogeneous systems should be allowed;
- the maximum network system functions should be provided to a user, with some degree of network transparency;
- a general purpose network with the capability for specific user applications should be provided. This will allow users the ability to expand those functional capabilities with the minimum impact.

In the operation of a network, McKay & Karp (1972:43) have identified two areas of great importance, namely:

- efficient utilisation of communication facilities; and
- overall network data management.

Lorin (1980:71-243) identifies the following aspects that should be considered when designing a computer network:

- communication costs;
- reliability;
- better user interfaces;
- security and privacy;
- capacity;
- system to fit organisation;
- hardware costs;
- operational costs; and
- application development cost.

Due to the nature and constraints of this paper these aspects are not discussed further, but it is important that they be noted.

Lorin (1980:22) also identifies important characteristics in a banking distributed computer system. These characteristics are:

- reliability and availability;
- quick installation;
- cost effectiveness;
- predictability of response times; and
- ability to grow with minimum disruption.

The Butler Cox Foundation held a seminar on strategic business services during March 1988 in Johannesburg. The presenter, Roger Camrass, presented a paper on Practical Networking Issues. He

identified the competitive edge as being very important, and stated that networks have contributed to competitive edge applications. He identified the following competitive edge applications that networks have contributed to:

Organisation/Sector	Competitive edge applications
- Retail	- point of sale (POS)
	- tracking newspaper distribution (database)
- Manufacture/distribution	- supporting franchises
	- just in time (JIT)
	- order collection (portable terminals)
- Services	- travel agent links
	- online proposals
	- online information.

Camrass (1988:35) has indicated that new network models are required in order to respond to changing business and system needs. He suggested that networks will have to evolve towards "open models" as interconnectivity becomes more important. The following elements are deemed important in network functionality (Camrass, 1988:57):

Network management

- Charging and traffic statistics; and
- Security and access control.

Information routing and handling

- Addressing and sequencing; and
- Formats and protocols.

User interface

- Applications interface; and
- End user interface.

Camrass (1988:112) has also stated that the following need be taken into account in network planning:

- Erosion of private networks;
- New technologies;
- New services;
- New management.

Once again, due to the purpose and constraints of this study, these aspects are to be noted, but cannot be discussed in detail.

Conclusion

A number of considerations are very important from a business perspective. The chapter dealing with the history of computer networks in this paper indicates that certain problems were already encountered and had to be solved in the early years of networking. These issues are still important today and can be summarised as follows:

- protocol;
- communication paths;
- undetected error rate;
- node (hardware) failure;
- transmission time;
- access; and
- network integrity.

Another aspect which conforms with the main goal of businesses, i.e. profitability and return, is the competitive edge that should be considered. This chapter has shown how networks contribute to the competitive edge.

CHAPTER 5 - CONTROL CONSIDERATIONS

1. Introduction

Mair et al. (1978:11,12) state that controls are needed to reduce exposures, and list the following exposures which are to be prevented, detected or corrected by controls:

- erroneous record keeping;
- unacceptable accounting;
- business interruption;
- erroneous management decisions;
- fraud and embezzlement;
- loss or destruction of assets;
- statutory sanction;
- excessive costs; and
- competitive disadvantage.

Halper et al., (1985:16-3) distinguish between internal accounting controls and operational or administrative controls. Internal accounting controls in the computer environment are further classified into two groups:

- application controls; and
- general or integrity controls (Halper et al., 1985:16-8).

Application controls consist of programmed procedures, and data security and access controls (Halper et al., 1985:16-9). General or integrity controls are divided into five main areas:

- implementation controls;
- program security controls;
- computer operations or administration controls;
- data file security controls; and
- system software controls (Halper et al., 1985:16-11).

Halper et al. (1985: 16-11,12) also identify disciplinary controls as those that are concerned with making sure that the basic controls continue to operate properly and that assets are safeguarded. Disciplinary controls are divided into:

- segregation of duties;
- custodial arrangements and supervision.

Davis et al. (1983:37) classify general controls into five categories:

- organisation and operation controls;
- application system development and maintenance controls;
- hardware and system software controls;
- access controls; and
- procedural controls.

Davis et al. (1983:167) state that application controls are used to prevent, detect, and correct errors and irregularities as transactions flow through the application procedures.

Three areas of control are identified as:

- data preparation and input or direct entry;
- processing; and
- output.

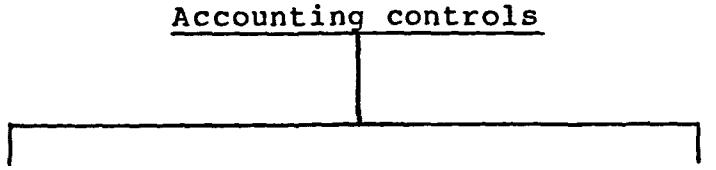
Halper et al. (1985:16-16,17) state that application controls are specific to programs that accomplish specific tasks. Application controls are divided into:

- completeness and accuracy of input;
- completeness and accuracy of update;
- validity of data processed;
- maintenance of data on files;
- calculating, summarising and categorising procedures;
- computer-generated data; and
- file creation and conversion procedures.

Bodnar and Hopwood (1980:475,476) describe the difference between general and application controls. General controls affect all EDP applications whereas application controls relate to specific applications. It is further stated that general controls are not a substitute for application controls. From the above it can be said that general controls control the environment in which data processing takes place and therefore the environment in which the application controls function. General controls are therefore necessary but not sufficient for adequate control over applications (Bodnar and Hopwood, 1980:476).

The controls mentioned above and their classification are graphically portrayed in figure 8.

Figure 8: Accounting controls in the computer environment.



General/Integrity/Environment controls	Application controls
Organisation controls	Completeness, accuracy of input
(Segregation of duties; custodial arrangements; supervision)	Completeness, accuracy of processing
Applications system development, maintenance and implementation controls	Validity of data processed
	Maintenance of data files
	Calculating, summarising and categorising procedures
Computer operations controls	Computer-generated data
Data file security controls	File creation and conversion procedures
Hardware controls	
System software controls	

2. Appropriateness of controls in a network environment.

As defined in chapter 1 of this study, a computer network system can consist of a variety of different devices at different locations, interconnected via a communications system. At the different locations a variety of different devices with different capabilities may exist. The different interconnected points may vary from large EDP installations to a simple input device. Due to the nature of a network system, new causes of exposure exist. Mair et al. (1978:391) summarise these causes as follows:

Type of System	Causes of Exposure
Remote Batch system	Loss of data
	Distortion of data
Remote Job Entry system	Loss of data
	Distortion of data
	Unlimited access
	Computer abuse
Switching system	Loss of data
	Distortion of data
	Delay of data
	Misrouting of data
Real-Time Inquiry system	Invasion of privacy
	Information not current
	Distortion of data
Real-Time Update system	Unlimited access
	Hardware/software failure
	Unsupportable results
	Human data-entry errors
Real-Time Programming system	Hardware/software failure
	Unsupportable results
	Human data-entry errors
	Computer abuse
	Destruction of programs
Data Base system	Unlimited access
	Destruction of files
	Software failure
	Slow response

Due to these new exposures new controls are necessary to control the processing and its environment and certain controls are emphasized to compensate for inherent weaknesses in the network environment (Watne & Turney, 1984:510). The previously discussed application controls summarised in figures 8 remain generally applicable in a computer network environment. Mair et al. (1978:391-398) identify various new controls for a network environment. These controls are classified as preventive, detective and corrective, and are summarised as follows:

New preventive controls

Passwords	: to control access
Physical terminal security	: to control physical access;
Authorisation	: to limit users to certain capabilities.

New detective controls

Line protocol	: to handle the variety of transmissions;
Up front edits	: to edit data before transmission;
Access logs	: to list attempted accesses, whether successful or unsuccessful;
Authorised user file	: to list the capabilities of every user;
Redundancy checks	: to detect distortions during data transmission (similar to parity check); and
Time control hardware	: to implement line protocol procedures; produce access logs; perform redundancy checks; and implement other security edits.

New corrective controls

Rotation of access	: to offset deterioration of preventive controls (e.g. passwords may become known);
Transaction log	: to recover data that were damaged or destroyed;
On-line instruction	: so called "help" function to assist users;
Recovery journal	: similar to the transaction log; it recovers over a shorter span of time; and
Graceful degradation	: to inform users of hardware and/ or software failures and provide direction for completing processing.

Halper et al. (1985:8-26) identify certain basic control areas that are important in any network system. These are the following:

Security of terminals and access;

Control over data;

Backup and recovery of the system;

General control considerations; and

Communication controls.

Certain new controls are necessary in these areas and Halper et al. (1985:8.26-8.30) identify the following controls in addition to the new controls identified by Mair et al. listed above:

Security of terminals and access

Disconnection of terminal after a number of invalid access attempts;

Disabling of terminal after being inactive for a predetermined period of time;

Periodical requests of password or other identification to authenticate users;

Critical information should not appear on the screen;

List of valid passwords should be protected against unauthorised access;

Entry of system commands that effect the status of terminals should be restricted to master terminals; and

System commands should be logged, reviewed and restricted.

Control over data

Reconciliation of control totals of transaction history file with totals of updated files; and

Memo updating of copy master files and comparison with updated actual master files.

Backup and recovery of the system

Maintenance of security copies of transaction history files and other log files;

Storage of critical system information, such as current network configurations; and

Dynamic back-out of partially-processed transactions.

As general controls control the environment within which data processing takes place, it is clear that general controls will be very important at every location in the network. Depending on the capabilities of each location, general controls will vary from location to location. If a particular location has application program development capabilities, obviously application program development, maintenance and implementation controls should be in place. On the other hand, if a specific location acts merely as an input terminal, application development controls would not be applicable. Every location will therefore have to be evaluated as to its functional capabilities so as to ensure that all the applicable general controls are implemented.

Halper et al. (1985:8-31,32) identify the following general controls that are very important in a network system:

Implementation controls

- application system design and implementation procedures are critical;

Program and data file security controls

- production, source and load libraries should be protected against unauthorised access;

Computer operation controls

- Only authorised jobs may be processed; and
- Development systems should be segregated electronically (or physically) from production systems;

System software

- controls over system software and especially communications and security software are essential.

Another important control aspect is that of physical access to communication lines. As the communications network makes it difficult to control physical access, the risk of unauthorised monitoring and/or modifications to messages exists. Security software and encryption techniques reduce this risk and often produce useful information (Halper et al., 1985:8-32,33).

Within a computer network system, distributed data processing may take place. The distributed data processing computer resources are decentralised and the decentralisation may include: distributed data; distributed software; and distributed system development and maintenance (Halper et al., 1985:8-33).

Distributed data processing systems are being used extensively, inter alia by banks and insurance companies (Watne & Turney, 1984:478). Distributed data processing systems have a major impact on control over data processing and Halper et al. (1985:8-35) and Watne & Turney (1984:478) identify the following areas of concern in a distributed data processing environment:

Security and access

- Security software may be degraded due to lack of appropriate memory and use of microcomputers; and
- due to space constraints or for other reasons, physical security procedures may not be appropriate to compensate for the above weakness.

Application controls

- decrease in specialisation and the lack of segregation of duties may require strong central supervision of locally-operated controls.

System development controls

- a lack of enforceable standards at local sites usually exists. Documentation is often insufficient or non-existent. Program changes are often not documented.

Halper et al. (1985:8-36) suggest the following ways to achieve a controlled distributed data processing environment:

- centralisation of system development;
- software controls over access to the computer, data files, and remote access control to the network should be implemented;
- physical access to the site should be limited;
- supervisory controls should be established;
- control information should be transmitted with data from one location to the other so as to enable the receiving location to reconcile control totals; and
- replicated files should be checked regularly for compatibility.

3. Conclusion

Computer networks introduce a host of new hardware and particularly new system software that need to be controlled. The more important new hardware introduced includes, amongst others, the following:

- terminals;
- modems;
- multiplexors;
- concentrators;
- communication lines;
- communication channels;

- communication control units; and
- front-end communications processors (Halper et al.,1985:8-9; Watne and Turney,1984:462; Lay and Eccles,1984:31).

As computer equipment is particularly reliable today, and hardware controls cannot generally be tampered with, these controls are less important than application, general, and especially system software controls. In addition to the existing operating systems, computer networks introduce the following system and supporting software which is to be controlled in particular:

- network control systems;
- teleprocessing monitor systems; and
- security control systems.

As all of these systems are generally parameter driven, the human factor plays an important role in the effective and controlled functioning of these systems. When evaluating controls in these systems, the systems and its controls should not be evaluated in isolation from each other, but should be seen as a "unit" and evaluated as such. The main object of controls is to limit exposures and risks, and these systems may in many instances complement each other, but there may exist weaknesses that should be compensated for by other methods.

CHAPTER 6 - CONCLUSION.

During the course of this study, it was realised that it is impossible to cover all relevant aspects of computer networks within the scope of the study. Inevitably, therefore, only some aspects have been attended to. Given this constraint, the study attempted to identify the more important business and control considerations in the design of a computer network. The more important business considerations identified, are:

the network configuration;
aspects of routing and flow control;
aspects of resource control;
aspects of data interchange;
aspects of telecommunications;
aspects of technical management;
costs;
effectiveness;
response times;
security;
accounting; and
the competitive edge.

The control considerations highlighted the new application controls needed and stressed the emphasis on general controls. It also highlighted new control areas due to additional hardware and system software. It can be stated that a computer network is a very complex

system which is exposed to a variety of hardware, software, and human risks. However,

> "when the proper controls are built in, the benefit of computer networks far outweigh any negative aspects such as security risks. In a well designed and controlled environment, such risks can be kept to a minimum" (Halper et al.,1985:8-37).

BIBLIOGRAPHY

1. STAMPER, D.A. 1986. Business Data Communications. 1st ed. Menlo Park : Benjamin/Cummings.

2. BACON, M.D.; STOKES, A.V. & BACON, J. 1984. Computer Networks - Fundamentals and Practice. 1st ed. Kent : Chartwell-Bratt.

3. WATNE, D.A. & TURNEY, P.B.B. 1984. Auditing EDP Systems. 1st ed. Englewood Cliffs : Prentice-Hall.

4. PAGE, J. & HOOPER, P. Accounting and Information Systems. 3rd ed. Englewood Cliffs : Prentice-Hall.

5. CHOU, W. 1983. Data/Computer Communications Network Structures. In CHOU, W., ed. Computer Communications. Vol. 1. Englewood Cliffs : Prentice-Hall.

6. WEIS, A.H. 1972. Distributed Network Activity at IBM. In RUSTEN, R., ed. Computer Networks. Englewood Cliffs: Prentice Hall.

7. McKAY. D.B. & KARB, D.P. 1972. IBM Computer Networks. In RUSTEN, R., ed. Computer Networks. Englewood Cliffs: Prentice Hall.

8. FRANK, H. 1972. Optimal Design of Computer Networks. In RUSTEN, R., ed. Computer Networks. Englewood Cliffs: Prentice Hall.

9. BEAUCHAMP, K.G. 1987. Computer Communications. Workingham: Van Nostrand Reinhold (UK)

10. LORIN H. 1980. Aspects of Distributed Computer Systems. New York: John Wiley & Sons.

11. CAMRASS, R. 1988. Practical Network Issues. London: Butler Cox Foundation.

12. HALPER, S.D.; DAVIS, G.C.; O'NIEL-DUNNE, P.J. & PFAU, P.R. 1985. Handbook of EDP Auditing. Boston: Warren, Gorham & Lamont.

13. MC LEOD, R. (Jr.).1983. Management Information Systems. 2nd ed. Chicago: Science Research Associates.

14. MAIR W.C.; WOOD D.R.; DAVIS K.W. 1978. Computer Control and Audit. 2nd ed. Altomonte Springs: The Institute of Internal Auditors.

15. PORTER, W.T. & PERRY W.E. 1981. EDP Controls and Auditing. 3rd ed. Boston: Kent Publishing Company.

16. WEBER, R. 1982. EDP Auditing - Conceptual Foundations and Practice. New York: McGraw-Hill.

17. LAY, P.M.Q. & ECCLES, M.G. 1984. The Principles of Business Computing. 2nd ed. Cape Town: Juta & Co.