

**INFORMATION SYSTEM AUDITING  
&  
DISTRIBUTED DATA PROCESSING**

An Analysis of Key Issues In Distributed  
System Audit Engagement Planning In  
Network Environment

Thesis Submitted  
for the Award of  
**Doctor of Philosophy**  
(Ph.D.)  
In  
**Management Studies**

By

**Mr. Jagdish Prasad Pathak**

Under the Guidance of

**Professor (Dr.) S.M. Bijli (Retd.)**

M.A. (Eco), M.COM, LL.B., Ph.D. (AMU), DND (The Hague), MRES. (London)

Former Head

Department of Com. & Management Studies,

&

Dean

Faculty of Com. & Management Studies

**Goa University**



Taleigao Plateau

GOA

March, 1993.

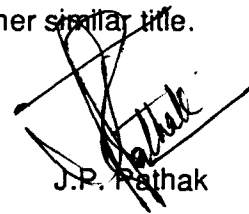
T-67

652  
PPT/IR

J.P.PATHAK.  
Department of Management Studies,  
Goa University,  
Taleigao Plateau,  
Goa - 403 001.

### STATEMENT BY THE CANDIDATE


I, Jagdish Prasad Pathak, hereby state that the thesis for the Ph.D Degree in Management Studies on, Information System Auditing and Distributed Data Processing; An Analysis of Key Issues in Distributed System Audit Engagment Planning in Network Environment, is my original work and that it has not previously formed the basis for the award of any Degree, Diploma, Associateship, Fellowship, or any other similar title.

  
J.P. Pathak

Place: *Altinho, Panaji (Goa).*

Date: *7/3/1993*

Countersigned by the Guide

  
*March 7, '93*



Professor S.M. Bijli  
M.A. (Eco), M.Com., LL.B., Ph.D. (AMU), DND (The Hague), MRES (London)  
Dean & Head (Retired)  
Faculty of Commerce & Management,  
Goa University,  
Taleigao Plateau,  
Goa - 403 001.

## **A B S T R A C T**

As the application of information technology has proliferated in business organisation and the technical complexity of computer based information system (CBIS) has increased, the importance of successfully auditing business usage of information technology expanded accordingly. In particular , the growing use of telecommunications network as an integral feature of modern management information system has resulted in requirements for advanced financial and administrative controls and for more sophisticated information system audit procedures. Large-scale, integrated networks have weakened the conventional mechanisms relied upon by auditors to control the risks associated with the traditional exposures. At the same time, the expansion of access to information system through computer networks has created entirely new exposures, thereby increasing the potential for unauthorised release of or tampering with proprietary system, and the information that those systems maintain.

Previous research has been conducted primarily from the relatively straightforward perspective of the single, centralized computer processing site. This research focus, while helpful in understanding CBIS audit processes in the context of individual processing system nodes, has not dealt adequately with the complex issues of auditing the distributed network-oriented information processing architectures that have become increasingly commonplace in modern business organisations.

Theses issues have spawned in this research a new model of information systems auditing. This model emphasizes the duality of auditing computer-based information systems that utilize both sophisticated computing and network facilities.

Based upon this theoretical model, a set of thirty seven variables relating to the process of planning CBIS audits were identified. A questionnaire was then developed and data collected from a diversified group of CBIS auditors employed by large multi-national accounting firms of Chartered Accounts, having a branch/franchise in India.

Two sets of critical success factors(CSFs) were identified in this research, those relating to planning for CBIS audits within traditional, mostly centralized computing environments and those related to such planning in complex computing and network environments. A comparison of the two sets of critical success factors was undertaken to develop an increased undertaking of the basic impact of technological change upon the effectiveness of the information systems audit engagement planning process.



## **F O R E W O R D**

In the historical domain of EDP auditing, by now the soundness of methodologies has been achieved, and if at all any conflict occurred, it was more to do with the application of methodologies rather than with the methodologies themselves.

It is this area of information systems auditing that is currently posing a great challenge to the auditors. This particular aspect of modern auditing deals with the methodologies for control and audit of computer based information systems (CBIS). The rate at which new and complex computing technologies and networking complexities has grown, seems to have converted most of the existing audit methodologies into obsolete ones.

I have made an attempt in this doctoral dissertation to analyse certain critical issues (called, key issues) in distributed systems audit engagement planning in network environment. This study is based on a theoretical model derived out of the review of existing researches and studies done. Though a profound number of theoretical studies were noticed while reviewing hardly 5-6 studies could be claimed to have been done empirically. I hope that this study would act as a catalyst for future researches and add to the realm of empirical studies in this super speciality area of management information systems.

I am indebted to Prof. Gordon B. Davis, Chairman, Watson School of Management, University of Minnesota; Prof. Ronald Weber, GWA Professor of Commerce, University of Queensland (Australia), and Mr. Charles H. Le Grand Mgr. (Adv Tech.). Institute of Internal Auditors Inc. Florida (USA), for responding to

my various problems pertaining to this research study and motivating me at the crucial stages to successfully complete this doctoral dissertation, apart from sending the required reference material.

I acknowledge with gratitude the authorities of the Indian Institute of Management, Joka - Calcutta, and the Institute of Cost & Works Accountants of India, Calcutta, for providing all the required reference material and software help during my couple of study visits. I must thank Dr. Mukherjee, Chief Librarian IIM; Dr. A. N. Dutta, Joint Director Research ICWAI; Dr. Vishwanathan, and Professor A. Bagchi - CAMC/IIM - Calcutta, for extending a helping hand during the critical phases of this research study.

I would like to express my indebtedness to Prof. M.C. Shukla, Prof. P.K. Ghosh, and Prof. M.K. Choudhary eminent authorities in Finance area at the Indian Institute of Planning & Management - New Delhi & Delhi School of Economics (University of Delhi) for providing me with a research environment and academic platform during my tenure as a Research associate at I.I.P.M. and subsequently as a lecturer in Commerce at University of Delhi.

Prof. (Dr.) N.K. Sharma, currently with North-Eastern Hill University - Kohima (Nagaland), Prof. (Dr.) S.N. Maheshwari, University of Delhi and Prof. (Dr.) Vaidya, former Head, Dept. of Computer Science & Technology, Goa University extended all possible help and gave me professional and academic opportunities to develop my stray thoughts into a finished thesis. I express my deep sense of gratitude to all of them.

I must thank Prof. (Dr.) Azhar Kazmi, Chairman, Faculty of Management Studies, Aligarh Muslim University who reviewed the entire manuscript of the thesis before the submission and whose detailed comments on various issues could give me a chance to enhance the validity of thesis.

I express my gratitude to the Chief Librarian, Shri Navelkar, and his associate Shri Bhuriye, and the faculty members of Department of Management Studies & Department of Commerce of Goa University for references and for participating in required discussions on different research issues from time to time.

My 'study-subjects' drawn from various metropolitan city offices of Arthur Anderson & Co., A.F. Ferguson & Co. Fraser & Ross, Deloitte, Halkins, & Sells, Price Waterhouse & Co., and Mc Kinsey & Co., deserve special thanks for responding in time and in sufficient strength so that the study could take a tangible shape.

Professor S.M.Bijli, my teacher, mentor, philosopher and guide, to whom I have no words to express my gratitude except the one statement that without him perhaps this dissertation could not have seen the completion. I simply bow to him in reverence.

In the end, my <sup>e</sup>parantes, my wife Nupur and my son Joy deserve my appreciation for the patience shown by them in bearing with my study for a long period.

Mr. Francis Gonsalves of Masons Communications, Panaji deserves special thanks for making available all the necessary software and hardware support to give a finished look to this thesis.

A handwritten signature in black ink, appearing to read 'Jagdish Prasad Pathak', written in a cursive style.

**Jagdish Prasad Pathak**  
D-4/2 Govt. Officer's Flats,  
Altinho, Panaji - 403 001,  
GOA STATE



# **C O N T E N T S**

I Statement on the Topic of Research.	i
II Abstract.	ii
III Foreword.	iv
IV Index	viii
V List of Sketches & Diagrams.	xi
VI List of Tables.	xii

## **Chapter 1**

### **INTRODUCTION 1-9**

**Information Systems Technology : A Revolution/Auditability of Networking :  
Some Issues/Audit Issues In Network Environment/Topics to be Investigated.**

## **Chapter 2**

### **REVIEW OF LITERATURE 10-47**

**Foundations of Computer Based Information Systems (CBIS) Auditing/The  
Effect of Evolving Technology/Need And Importance of Computer Communica-  
tion/Audit Practices In Information Systems/Factors Affecting Auditor's  
Judgement/Computer Network Auditability.**

## Chapter 3

### THEORETICAL FOUNDATION 48 - 74

Overall Research Paradigm/Audit Cycles/Critical Success Factors/Audit Engagement Planning Process : General Model/Controls Complexities/Theoretical Model: Part I - CBIS Audit Requirements/Part II-CBIS Audit Resource Allocation/Part III - CBIS Audit Procedures/Theoretical Model: In Brief/Research Questions.

## Chapter 4

### RESEARCH DESIGN & METHODOLOGY 75 - 100

Research Strategy & Design/Data Collection Instrument/Research variables - Understanding of Audit Requirements-Breadth of Training - Depth of Training - Breadth of Experience - Dept of Experience - Availability of Audit Tools - Quality of Professional Judgement/Data collection & Analyses - Assessing Component Differences - Determining Component Criticality - Extracting Critical Success Factors - Comparing Technical Environments/Summary.

## Chapter 5

### ANALYSES AND INTERPRETATIONS 101 - 163

Research Subjects/Paired Responses Between Scenarios/Criticality of Component Variable/Appropriateness For Factor Analysis/Scenario A: Critical Success Factors - Factor 1:

Computer Modeling Capability - Factor 2: Information Technology Specialisation  
- Factor 3: Computer/Networking Technical Training-Factor 4:Computer/Networking Technical Experience - Factor 5: Advanced Technical Systems Expertise  
- Factor 6: CBIS Audit Engagement Management - Factor 7: Traditional Financial Accounting Background - Factor 8: Traditional CBIS Audit Skills - Factor 9: Technical Reference Library - Factor 10: Standardised Audit Methodologies-Factor 11: Information Systems Management Training/Scenario B: Critical Success Factors-Factor 1: Computer/Networking Technical Experience - Factor 2: Information Technology Specialisation - Factor 3: Computer/Networking Technical Training-Factor 4: Traditional Financial Auditing Background - Factor 5: CBIS Audit Engagement Management-Factor 6: Advanced Networking Expertise - Factor 7: Standardised Audit Methodologies - Factor 8 : Audit Planning Flexibility-Factor 9: Coordination with Financial Audit Staff/Criticality Measures For Factors/Critical Success Factor Ranking.

## Chapter 6

### DISCUSSION OF FINDINGS 164 - 183

Summary of Results/Theoretical Factor Constructs/Comparison of Scenario A and Scenario B Factors/Implications of this Research/Limitations & Future Research Directions/Summary & Conclusions.

### BIBLIOGRAPHY 184 - 210

### APPENDIX

#### I Data Collection Instrument

## **List of Diagrams/Sketches/Flocharts**

### **Figure**

**2.1 : Categories of CBIS Controls.**

**3.1 : An Audit Cycle.**

**3.2 : Planning Echelons For CBIS Audit Engagements.**

**3.3 : Information Systems Controls Grid.**

**3.4 : Developing CBIS Audit Requirements (Computer).**

**3.5 : Developing CBIS Audit Requirements (Network).**

**3.6 : Planning CBIS Audit Resource Allocation.**

**3.7 : Determining CBIS Audit Procedures.**

**3.8 : Planning CBIS Audit Engagements.**

## **List of Tables**

### **Table**

- 4.1 Candidate Factor Reference Summary.**
- 4.2 Composition of CBIS Audit Resource Planning Factors.**
- 5.1 Summary of Respondent Demographic Data.**
- 5.2 Summary of Respondent Work History.**
- 5.3 Respondents Self-Reported levels of Expertise.**
- 5.4 Pairwise T-tests Between Scenarios A and B.**
- 5.5 Criticality Index For Scenario A.**
- 5.6 Criticality Index For Scenario B.**
- 5.7 Factor Determination From Scenario A.**
- 5.8 Scenario B Factor Determination.**
- 5.9 Scenario A Factor 1 Criticality.**
- 5.10 Scenario A Factor 2 Criticality.**
- 5.11 Scenario A Factor 3 Criticality.**
- 5.12 Scenario A Factor 4 Criticality.**
- 5.13 Scenario A Factor 5 Criticality.**
- 5.14 Scenario A Factor 6 Criticality.**
- 5.15 Scenario A Factor 7 Criticality.**
- 5.16 Scenario A Factor 8 Criticality.**
- 5.17 Scenario A Factor 9 Criticality.**
- 5.18 Scenario A Factor 10 Criticality.**
- 5.19 Scenario A Factor 11 Criticality.**

- 5.20 Scenario B Factor 1 Criticality.
- 5.21 Scenario B Factor 2 Criticality.
- 5.22 Scenario B Factor 3 Criticality.
- 5.23 Scenario B Factor 4 Criticality.
- 5.24 Scenario B Factor 5 Criticality.
- 5.25 Scenario B Factor 6 Criticality.
- 5.26 Scenario B Factor 7 Criticality.
- 5.27 Scenario B Factor 8 Criticality.
- 5.28 Scenario B Factor 9 Criticality.
- 5.29 Scenario A Factor Rankings.
- 5.30 Scenario B Factor Rankings.
- 6.1 Comparison of Scenario A Factors.  
    With Theoretical Factor Constructs.
- 6.2 Comparison of Scenario B Factors  
    With Theoretical Factor Constructs.
- 6.3 Scenario A & B Critical Success Factors.

# CHAPTER 1

## INTRODUCTION

Computer and its varied uses has proved phenomenal and dramatic growth in the use of information technology in India and elsewhere in developing countries for the past 2-3 decades. This growth continues to raise numerous and difficult managerial and technical questions. Consequently, there is an ongoing need for systematic scientific-research to address these questions to in providing clear insights into this fast changing and increasingly complex technology, and its application in modern business organisations.

A wide range of significant questions that could provide specialists in Management Information System (MIS) with research topics, are being generated by the expansion of the use of Computer Communications in information systems. These topics are not only numerous, but important also. One such research topic relates to the process of auditing Networking applications and facilities [Amoroso (1986); Beath (1986)].

The topic for this thesis is the application of information systems auditing techniques to distributed data processing including an analysis of key issues in distributed systems audit engagement planning effectiveness in network environment. The objective of this study is to add to the base of knowledge and research ever growing in the field of Computer based information systems (CBIS) auditing. The focus of this chapter is on introduction of the nature of research that is described in this thesis. The chapter begins with a discussion of the current 'revolution' in the information systems technology, so as to provide a general background for this research. Subsequently, several issues in the area of distrib-

uted systems auditing spawned by this technological revolution are presented. The chapter concludes with a brief statement of the questions related to computing and networking audit effectiveness that are to be investigated during this research.

### **Information Systems Technology : A Revolution**

Synott & Gruber (1981) seem to be justified in referring the telecommunications as the "enabling technology" that allows information systems to be integrated into a cohesive whole that will meet the needs of organisations. The International Standards Organisation defines tele - communications as the "transmission of signals over long distances" [ANSCIPS (1982)]. These terms 'telecommunications' and 'networking' are used interchangeably to refer to voice or data communication, or both, as appropriate, in this thesis. The biggest contribution of the fast evolving microprocessor technology has been in the advent of very small, very fast and amazingly inexpensive logic and memory devices. These are being used as building blocks in a myriad of computing and networking applications (including LAN and WAN) [Russo (1983); Witten (1983); Parker et al (1987); Beguai (1986)]. Microprocessor is used to operate large and small computers, communication devices of all kinds, and 'intelligent' and 'dumb' terminals alike.

The advent & development of the personal computer (PC) is having a profound impact upon organisations. Though the demand for PC's began to level off during the late, 80's, a surge in the demand for mainframes and minicomputers continues to be strong [Business Week (15/7/85); Datamation (15/5/85)]. The tremendous acceleration in the growth of telecommunication traffic will continue, as Government of India (who controls tele-com), and industries which recog-



nise the need to inter-connect their micro Computers, mini Computers, and mainframe Computers to achieve distributed processing and office automation objectives [Uhlig, Farber, And Blair (1979); Kimbel (1987); Kay (1986); Hufnagel (1987)]. There is much more to this phenomenon than the growth in usage of various forms of electronic technology. Powerful economic forces are causing these trends [Diebold (1985); Lecht (1977); Stix (1987); Withington (1987)].

Historically, the separation of telecommunications and Computer networking technologies [e.g. Local Area Network (LAN); and Wide Area Network (WAN)] was based upon industry structures that characterized voice telephone services as a regulated monopoly of Govt. of India, Dept. of Telecom; and Computer industry as unregulated and highly competitive. The developments of microprocessor as functionally programmable digital component that can, and is being used in all forms of network, as well as computing, has highlighted the inappropriateness of continuing to maintain legislated separation of computing and networking into two separate entities even in the U.S.A. Synott and Gruber (1981) have even coined the term 'Computications' to emphasize the merging of the Computer and telecom industry in the U.S.A.

Until recently, the use of digital technologies was profuse only in computing applications. But networking applications were few & rare. However, the various amalgamations, mergers and Japanese electronic development are causing a revolution in networking even in the U.S.A. [Young (1987); Andreychuk et al (1987) Sape (1991); Singhal et al (1989)]. In India, we still lag behind in this direc-

tion to an extent. Satellite, microwave, and optical fiber communications media are all proliferating; however, traditional analog communications electronics and land-lines are still the dominant media in telecommunications due to the vast capital investments. Govt. of India/P & T Dept. has been slow to change, but now corporatisation of P & T Dept. as Mahanagar Telephone Nigam Ltd. (MTNL) in Metropolitan cities of India, is slowly changing that situation. As the telecommunications evolve, the future will belong to fiberoptics operating in a digital mode & integrating audio, video, and data communications. Both, private based and public switched networks will gravitate toward optical media as the part of the digital revolution in telecommunication sector in India [Raymond (1987); Potter (1987); Spooner (1987); Pathak (1991); Walko (1988a, 1988b); Finnie (1985); Mc Inerney (1987)].

LAN and WAN are the latest in a long line of systems concepts that have captured the imagination of the Computer industry. These networking technologies are important developments in data-communications [Stallings (1984); Cho (1986); Young (1987); Read (1989); Jaikumar et al (1986); Pitroda (1988)]. It has crossed its infancy and maturing very rapidly, and may hold critical importance for future distributed computing applications and data-bases [Withington (1987); Stix (1987) Avison et al (1991, 1988)].

Computer branch exchange is another technology that could help inter-connect the office of the future [Mier (1985)]. This is a digital switch that allows the integration of voice and data communications on one network. The extent of actual integration varies, but in its most sophisticated form, digital telephones fully share the same lines with digital Computer terminals and other digital

equipment [Pathak (1988,1991)].

The network including logic components called 'Intelligent networking' can provide integrated network management capabilities, and it became a reality at the end of the last decade. Some intelligent network products are now on the market [Pocek (1985) Albert et al (1992); Allen (1992); Auramaki et al (1992)]. Such intelligent logic based systems will help to monitor and control network operations more effectively than with the comparatively crude tools that have been previously available in India and elsewhere in developing countries.

Taking into consideration the profound changes in telecommunications technologies area and considering their rapid expansion in the use of these technologies by the organisations, it is justified to be concerned because such developments may impair the effectiveness of auditing the computer based information systems with its proliferation. Many issues are surfacing as key ones; and these are described below.

### **Auditability Of Networking : Some Issues**

Majority of trends underway will change the ways in which organisations conduct their businesses, and the ways in which auditors conduct audits. The pervasive nature of information technology, the favourable economics and functional versatility of modern micro-processor based systems, and the competitive market forces that drive the rate of technological evolution are all favouring an era of profound change in the work-place [Bell (1973); Diebold (1985); Martin (1981b)]. The potential for the misapplication of information systems technology has increased correspondingly.

The issue of networking is least well understood by the management in general within information systems technology. The topic of networking is often the most pervasive for individual workers and most wide-ranging across organisational units of an enterprise. It is not only the approaches to networking technologies undergoing revolutionary change, but the needs for increased networking capabilities to support organisations information requirements are too, multiplying at the same time [Hiltz and Turoff (1978); Institution of Engineers (India) (1989); Bhat & HariGopal (1991); Ghosh (1989); Padmanabhan (1989); Bhattacharyya & Mitra (1991)].

The organisations will face the challenge to establish the management expertise and control mechanisms necessary to successfully implement new networks that can accommodate the onslaught of information technology during the remaining period of this century [Davis & Wetherbe (1981)]. Effective and efficient telecommunications systems are going to be needed to support and to interconnect at least the following units [see, Davis & Wetherbe (1979)].

1. Distributed Processors;
2. Office automation devices;
3. Integrated voice/ data/ video machines;
4. Intelligent work stations for managers, engineers, Secretaries, administrators, factory workers, scientists; and
5. Centralised data bank facilities.

These kinds of networks will affect the information systems audit process, at

least, by requiring the understanding of the integration of computing and networking functions by the auditor [De Witt et al (1992); Deen et al (1988); Potter (1987); Potter & Perry (1984)].

At this juncture of evolution in information technology, the risks associated with uncontrolled, poorly planned and operated networks, cannot be easily over-emphasised. The basic restructuring of jobs implied by the use of this technology, the levels of personal commitment and organisational disruption required to make such fundamental changes in business process changes, and the costs associated with installing and operating the new networking architectures will demand careful attention to management and operational control issues [Davis and Wetherbe (1981)]. The geographic dispersion of information systems access capabilities also indicates that better attention to access control may be warranted [Madnick (1978); Parker & Nycom (1984)].

Lastly, the increasing dependence of organisations on the use of Computer technology as a result of improved access to information through networking and distributed processing means that previous information systems exposures may be heightened significantly. These may achieve new levels of materiality in the audit process and prompt an ongoing re-examination of the assumptions underlying the content of each audit. The issues explored above as an individual or in combination could critically influence the information systems auditing process as it may be operationalised in a specific business situation. These issues raise many important questions about the application of this technology in organisations, individually and collectively.

## **TOPICS TO BE INVESTIGATED**

**A research study was undertaken to address the following general questions based upon the issues discussed above :**

- 1. The increasing usage of networking in information systems implementations affect information systems auditing. How?**
- 2. There are critical factors that influence effectiveness of an information systems audit in a complex computing and networking environment. What are those?**
- 3. How do the factors that influence information systems auditing effectiveness change in response to changing technology?**

**The answers to these questions should help information systems auditors to adopt and expand their auditing techniques and to update their auditing methodologies more effectively in order to deal with the new telecommunications component of Computer based information systems auditing. Such adaptations are required as sophisticated, integrated, and highly complex information systems environments have become common place in business and industry.**

**The present research has addressed the audit planning process for information systems audit and entails three different, but related, research efforts. The first is a field study undertaken to determine certain key factors that contribute to auditing success, those that are associated with CBIS audit planning in traditional information systems environments from the perspective of the professional CBIS**

auditor. The second is a similar field study to determine key factors for advanced CBIS environments with complex networking facilities. The third study is an analysis of the findings of the first two studies and a comparison of the differences and similarities between the two sets of factors identified. This comparison provides the basis for assessing the extent to which the two kinds of CBIS environments may require different approaches to achieve effective auditing.

## **CHAPTER 2**

### **REVIEW OF LITERATURE**

The effective auditing of complex computing environments making profuse use of telecommunication networks need the related critical issues to be researched and analysed empirically. The theoretical basis of this research is developed by drawing the relevant observations and summaries of prior research done in the relevant areas. Research results from the existing literature in the mutually related areas are analysed. For example, Management Information Systems, Financial Auditing, Computer-based Information Systems Auditing, and Computer Science were the chosen areas for this prior research results analyses.

The review of literature for this research consisted of examination of inter-related topics and issues. Each one of these is presented in a separate section of this chapter that follows.

Theoretical and practical foundations of Computer-based information systems auditing from the financial auditing, management control, and operational control view-point are presented in the first section of the review. Likewise, a review is done of the research literature that deals with the impact of changing information systems technology on the information systems auditing process. The scope of the review of impacts of technological change is extended in the third section of this chapter. And, the rapidly growing importance of Computer communication is examined as it relates to the CBIS auditing.

The literature on current information systems audit practices is summarised in



fourth section, including the factors contributing to the overall effectiveness of an audit. As an epilogue to the discussion of audit practices, a review is presented in the fifth section on auditor's judgement, finally, the last section is meant to synthesise all the presentations made in earlier sections of this chapter and presents a brief summary of the researches done in the area of computer network auditability.

Apart from some of the conceptual/theoretical researches in the area of auditing the distributed information systems, very limited empirical research is done in this field. But, it has been possible, by examining the literature from the various related fields, as explained earlier, to develop a base for support to the proposed research in the academic and professional literature. Next sections of this chapter, therefore, presents that basis of support.

### **Foundations of CBIS Auditing**

Operational controls and management controls form the part of total control activities of business organisations [Withington (1987); Walko (1987); Anthony (1965); Pathak (1991)]. Over the past 30 years, EDP has evolved the nature of these controls by the introduction of sophisticated computer technology as an integral and rapidly growing component of the structure of management and operational control in organisations [Davis (1960); Davis et al (1981); Mullender (1991)].

Management is charged with deciding how control of these resources, with regard to information resources will be affected and how performance will be assessed [Allen (1982); Perry & Warner (1978); Pathak (1991); Wolinsky et al

(1992); Igarria et al (1991)]. EDP audit or computer-based information systems (CBIS) audit is one of the techniques used by management to evaluate its own use of computer and telecommunications technology [Davis (1974); Dean (1968); Mc Farlan (1973); Nolan (1982); Pipino (1978); Reuter (1985); Pathak (1988); Igarria et al (1992)].

It is basic for both financial and EDP auditors to understand financial control systems in a particular organisation. Modern business systems using complex and evolving nature of computer technology, are very difficult to audit [Davis et al (1983a); Perkins (1983); Van Zutphen (1980); Pathak (1988); Lederer et al (1992) Clark (1992)].

However, a general conceptual framework for audit process has been developed by the professional accounting organisations and this paradigm provides the professional structure within which CBIS auditors are expected to function [Weber (1984); Porter et al (1984); Davis et al (1983); Pathak (1991)].

The concept of "internal control" in any organisation is the principal focus of this paradigm [Horngren (1982); Gordon et al (1969); Lucas (1989); De Witt et al (1992)]. The official professional definition as provided by American Institute of Certified Public Accountants (1976) of internal control is given below :

"..... the plan of organisation and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency and encourage adherence to prescribed managerial policies."

The evaluation of systems of internal controls in an organisation is one of the main activities of any audit. The extent of reliability of existing internal control systems is determined by the auditor as the basis for the audit. Auditor also makes use of that determination to extend or limit the scope of subsequent audit tests. The depth of test is further decided by the professional judgement of auditors based upon the specific situation under examination [Mair et al (1972); Carlson (1982); Brown (1983); Pathak (1988 & 1990)].

AICPA (1977) provides only two controls, viz., internal accounting controls and internal administrative controls. Internal accounting controls consist of all those methods used to safeguard assets and maintain the reliability and integrity of financial records and statements. Internal administrative controls include the processes by which management makes its decisions and the methods used to obtain the compliance with its non-accounting policies. These two categories of internal controls are further sub-divided into two groups each. The first two groups include financial accounting controls and EDP accounting controls. The second two group includes financial administrative controls and EDP administrative controls.

EDP controls are summarised as follows [Davis et al (1983) :

**"EDP Accounting controls include the segregation of EDP functions; EDP controls to ensure that only authorised transactions are processed using authorised computer programmes; EDP controls to ensure complete, correct, and timely recording and processing of transactions; EDP access controls; periodic comparison of stored data with assets and establishment of regular procedures to compare the physical counts, records from parties outside the organisation and other**

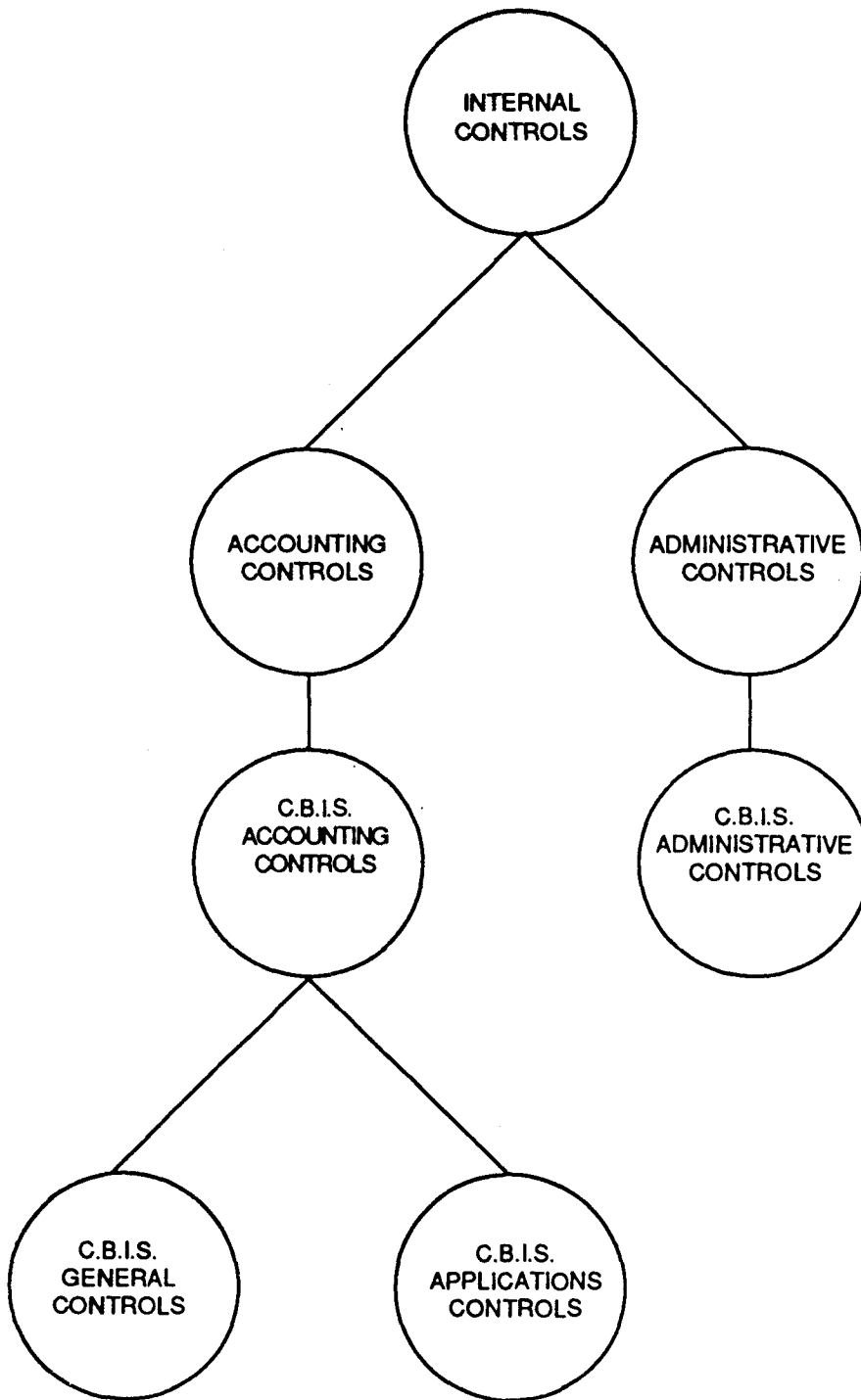
evidence of assets.

**EDP Administrative controls** ensure that useful information, is provided and used in achieving the organisations objectives. Controls to ensure efficiency in operations are also part of administrative control.

Consequently, EDP accounting controls are divided into two classes depending upon the scope of each individual control technique, called general controls and application controls [AICPA (1978)]. General controls are those global EDP accounting controls that are associated with all EDP activities in the organisation being audited. Application controls are the EDP accounting controls that apply to specific automated accounting application systems. Figure 2.1 depicts the relationships between these various categories of controls.

Auditors (both, financial & CBIS) can be either external or internal. External auditors are the outsiders, brought into an organisation to provide an objective professional opinion as to the financial conditions of a business. The AICPA (1977) permits the external auditors to limit their examinations to internal controls in accounting. Internal auditors, conversely, are the insiders, employed by the organisations that they audit. Internal auditors examine both internal accounting controls and internal administrative controls. The internal auditor provides management with a key element in the organisation's feed-back control loop [Thomas (1992); Horngren (1982); Pipino (1978)]. Somewhat similar to AICPA guide-lines, Indian counterpart i.e. ICAI too has suggested the professional standards in this field.

**Figure 2.1**



**CATEGORIES OF C.B.S.I. CONTROLS**

'Audit reliance' can be placed by the internal or external auditor upon the output of the systems only after thorough examination of computing environment of a company and after determining the adequacy of EDP general as well as application controls. The reliance on the outputs of the system for financial audit purpose is not justified, if the auditor is not convinced of the completeness or reliability of EDP controls [Brooke et al (1983); Camrass et al (1987); Carlson (1982); Brill (1982); Brown (1983); Weber (1986)]. The use of computer in the audit process by the auditor in varying situations and circumstances is referred to as 'auditing through the computer' and 'auditing around the computer'. Although as Davis (1968) points out that such terms tend to be misleading, but on the same hand do show two equally important philosophical approaches to financial auditing of organisations that rely upon computers to process their financial data.

Davis (1968) only remarks further that a typical non- technical financial auditor more often than not prefers to audit around the computer. In this way, the unexpected computer errors can be controlled without requiring to rely upon an in-depth understanding of computer technology. However, the increasing use of information systems technology in organisations, combined with other factors described below, is causing this approach of auditing around the computer less effective and even eventually obsolete.

### **The Effect of Evolving Technology**

Auditing process of Computer Applications and Computer Operating environments within business Organisations is acquiring more importance and more complexities [Allen (1982); Davis & Weber (1983b); Davis & Wetherbe (1981);

Diebold (1985); Mc-Farlan et al (1983); Perry (1985); Weber (1984); Weiss (1980); Davis C.K. (1986); Lockwood et al (1989); Deen et al (1988)].

This situation is aptly summarised by Branscomb (1979), the Chief Scientist, IBM Corporation as below :

**"People are always asking, ' in the world of the future, will information systems be centralised or decentralised, maxi or mini, top-down or bottom-up?' My answer to all such things/questions is 'Yes'.. even within a single user organisation, there may be multiple systems having different structural characteristics or having subsystems which are structured differently."**

For CBIS auditors, this statement amply illustrates the growing challenge. The fast increasing diversity and complexity of information systems technology will increase the difficulty of auditing these systems effectively [Davis and Weber (1983a); Parker (1981); Perkins (1983); Porter & Perry (1984)]. Further-more, the spread of information systems technology simultaneously increases the importance of achieving effective audits for the purpose of supporting management controls [Carlson (1982); Parker (1984); Pipino (1978); Wysong (1983); Hull et al (1991); Ling et al (1992)].

The turnaround achieved by a company is well reflected in the way it uses computer resources [Padmanabhan (1989); Walko (1988a); Gibson et al (1974). The reflection of the use of Computer begins to show up and to spread out into the Organisation. The organisational function shifts from an EDP paradigm to a MIS paradigm. As the research related to the application of stage theories to the

usage of computing systems in organisations attests, this transition from EDP to MIS is a difficult one for Organisations to make [Nolan (1979); King and Kraemer (1984); Benbasat et al (1984); Pathak (1990)].

The shifts in these organisational paradigm imply that corresponding and difficult transitions are needed in the information systems audit function to match the organisations as they evolve [Porter & Perry (1984)]. The proliferation of computing technology including large scale computers, mini- computers, micro-computers, data communications networks, local area networks, wide area networks, time-sharing terminals, intelligent work stations, and related technologies such as voice, video, and fascimile processing and transmission, has greatly affected the internal controls relied upon by businesses to manage organisations and by auditors to review them [Davis & Weber (1983b)]. The following problems in internal control associated with the use of computers in businesses have been noted by Hooper and Pate (1982) :

1. Source documents are eliminated;
2. Information is changed without physical trace;
3. Sophisticated tampering can cause unauthorised actions;
4. Computer speeds can increase even one persons Capabilities dramatically;
5. Expanding system capabilities change the underlying business reality;
6. Records and audit trails are invisible;
7. Organised, summarised, and concentrated information is easier to steal;
8. Computer-based information is easier to lose;
9. Computers provide new sources and potential for errors;



10. Individual and group work activities and products of otherwise segregate duties are consolidated in computers;
11. Computers lack judgement;
12. Users are nevertheless in awe of computers and networking technologies.

All these issues are affecting the ways that auditors must operate in order to be effective in evaluating information systems that utilise computers [Davis & Weber (1983a); Wilkinson (1978); Burns et al (1992)].

It was found in a study by Lampe et al (1984) of auditor's assessment of potential exposures that the evaluation of internal controls got changed due to the use of distributed processing technology. It so happened due to the presence of enhanced exposures, introduced by the technology itself.

Computers are becoming basic tool for use in conducting audits as advanced, increasingly integrated computing systems replace older less complex data processing environments. [Bailey et al (1978); Lord (1975)]. Auditing through the computer will increasingly become the most feasible approach to conducting/financial audits [Litecky et al (1981)]. The need for audit reliance upon the outputs of complex computer environment utilising distributed processing, integrated data bases, and sophisticated data communications networks will increase [Porter et al (1984)]. The personnel reviewing such complex 'total systems' environments of the future must have the training and proficiency needed to routinely evaluate advanced computing and networking technology [AICPA (1978); Perkins (1983); Auramaki et al (1992); Avison et al (1991)].

## **Need & Importance of Computer Communications**

Various forms of data communication are used to link the computers together. These are put to use primarily to facilitate the authorised sharing of data, and accomplished use of communication technology. The architecture in which decentralised systems are inter connected using communications technologies is, of course, distributed processing. Computer Communications are significant components both of distributed processing and of office automation systems (OAS) architecture. It has become essential to establish a total systems frame of reference, with the decentralised computer systems. It means to recognise the effects of the technology on the human aspects of the information systems environment and to view the organisational changes that result from technological innovations with realistic understanding of the impacts of such changes throughout the host organisations [Bostrom et al (1977 a)]. New controls are required to manage decentralised computer environments [Burnett et al (1975)]. The distribution of processing includes with it the distribution of responsibility for information handling [Withington (1980)]. On the same hand, there are strong reasons to favour maintaining a central authority that is responsible for the overall information systems environment including the data communications network and other organisation wide facilities [Davis et al (1981); Holland (1982); Mekenny et al (1982); Burton (1987); Verrijn-Stuart (1987)].

Apart from the proposition that organisation-wide facilities should be controlled centrally, there are technical reasons to support the current widespread centralisation of network controls. While the accuracy, privacy, and security of data handled locally must ultimately be a local responsibility. Networks, which are controlled centrally are more likely to be auditable because the large storage

capabilities at central site can better capture and maintain detailed transaction data needed for conventional computerised logs and the detailed audit trails for networking facilities [Holland (1982)].

The information systems manager initiates organisational change by directly influencing the technology for handling information [Nolan (1973)]. Presently, a number of distributive technologies are available, from personal computers and office automation systems to mini-computers and large mainframe oriented networks. The user communities have acquired the capability to use particular information technology as a tool for change that is essentially under their control [Folger et al (1983)].

The influence of the organisational information systems manager on the others in the same entity is indirect. The traditional systems controls are not necessarily utilised in a distributed systems environment [Burnett et al (1975)]. The problem for the information systems auditor is that the traditional centralised facilities with which auditors are most familiar, are competing with the user organisations desires for increased autonomy and control over information resources [McKenney et al (1982)].

The basic forces behind the decentralisation of computing resources are the desires and the underlying needs driving information systems auditors toward distributed processing. The decreasing costs associated with the micro processor technology, too gives impetus to the desire [Davis et al (1979)].

The audit characteristics similar to those of a centralised mainframe facility are

found in each individual node of a distributed computer network [Hirschheim et al (1988); Jancura et al (1983)]. Individual nodes of a distributed computer network, in general, do not pose any problems for the information systems auditor, although those tend to increase the amount of audit work that must be done in a distributed environment with multiple sites. The evaluation of exposures is a critical audit issue that can arise from the ways in which nodes are linked together either organisationally or technically [Hull et al (1991); Burns et al (1992); Ling et al (1992); Allen (1968); Davis et al (1983); Lucas (1983)]. Effective auditing of the Computer Communications networking facility is central to recognising and dealing with many of these kinds of exposures [Trotman et al (1985); Weber (1982); Avison et al (1988)].

The complexities of internal control mechanisms and compliance testing techniques increases with the proliferation of distributed systems technologies in its various forms, viz., office automation systems, distributed data processing, and integrated telecommunications networks [Van Zutphen (1980)]. Later on, Dickson and others (1984) identified the importance of these complex integration problems and subsequently emphasised it in their study.

The implementation of computer based information systems is generally expected to improve communication and control within an organisation, but changes in one area can create unexpected effects on other manual or automated systems within the organisation [Bostrom et al (1977 b)]. As Computing is decentralised, each installation of a distributed system is essentially a large scale computing system in miniature [Davis et al (1981)].

This kind of decentralisation in different parts of an organisation gives rise to rapidly shifting priorities [Mc Farlan et al (1983)]. Such rapid shift implies that controls will be difficult both to sustain and to maintain and that CBIS auditing practices in this kind of environment will require adaptability and flexibility.

While, dealing with such complex distributed systems environments, a CBIS auditor will be required to have a high level of technical sophistication [AICPA (1978); Vaneck et al (1983); Van Zutphen (1980); Weber (1980)]. All levels of organisation and each processing node of distributed network will potentially need a CBIS audit function [Davis et al (1979); Wooding (1984)].

A growing awareness is fostered by the decentralisation of systems that the linking of these decentralised systems is an important stage in the development of the information infrastructure within organisations [Davis et al (1981)]. A vital component of CBIS auditing practices will contain the techniques associated with effective auditing of telecommunications facilities [Davis et al (1979)].

However, a study describes that the approaches and techniques currently being used by many auditors are simply not very effective in a decentralised environment, one that uses telecommunications and data integration [Porter et al (1984)].

The information systems auditing practices in most of the cases are outdated. It has so happened that most data processing systems operating today are based upon earlier generations of mostly manual systems and that such systems tend to show the characteristics and controls of those previous generations. Even after

accepting that information systems auditing as practical today is fully adequate, it is reasonable to expect that the ongoing growth in the use of telecommunications by itself will mandate a major restructuring of information systems controls and audit concepts [Weber(1984)].

A study conducted by Ball and others (1982) identified the priorities of top management. They found that 'gauging MIS effectiveness' was ranked second, just behind information systems planning. It was also found out that the primary function of CBIS auditor is to assess the MIS effectiveness. As noted by [Diebold (1985)], the growth of sophisticated telecommunications systems in business continues to far exceed expectations, even as those expectations have increased considerably over time.

It is the decentralisation of computing in organisations which inturn appears to change the CBIS auditor's functions, in brief. An audit that gives too much attention to reviewing individual computer applications is not considered to be sufficient. More than ever before, a total systems perspective is required to direct the CBIS audit processes.

The application of improved controls is becoming essential that deal with telecommunication of networks. Decentralisation of computing inherently stretches the scope of the CBIS audit and correspondingly increases the depth of activity outside the information systems departments. Therefore, CBIS auditors need to expand their knowledge of telecommunications, and information systems technology. They are to deal effectively with the ongoing influences of technological change on business organisations and, indirectly on their auditors. These chang

es include wide- ranging decentralisation of computing capabilities, increasing complexity of systems, growing organisational dependence upon the technology, shifting priorities in the application of the technology, and rapid expansion in the utilisation of communications technology as integral components in information systems architectures of all kinds.

The final part of the review of literature presented in the succeeding section deals with the auditability of computer networks. A review of existing CBIS auditing practices is made and the issues pertaining to auditors judgement in the CBIS auditing profession are described as a basis for a subsequent review of the literature dealing with the network auditability and the changes in auditing practices being dictated by the revolutionary changes in the ways that organisations use information systems technology.

### **Audit Practices In Information Systems**

During the last decade of 80's, the auditing of computer based information systems in organisation has been actively pursued. Generalised CBIS auditing methodologies evolved during this period only to help structure the auditing process [Pathak (1990)]. The objective of this section of the literature review is to summarise the literature that relates to generalised practices in the auditing of the use of information technologies.

Audits are conducted by individuals or by audit teams [Davis (1974)]. Audit teams are often used because of the division of labour and resulting specialisation in the evaluation of complex information systems environments in the audit [Van Zutphen (1980)]. In either the individual or team situation, the ability of the

team or that of the individual, determines the effectiveness of an audit engagement. In the discussion that follows, the term "auditor" is used to refer to the individual or to the team functioning as a unit, as appropriate.

In general, there are two kinds of CBIS audit approaches, viz., review of data and evaluation of system controls [Glieznner (1985); Perry et al (1978)]. Reviewing data involves extracting, summarising, and reporting on "production data to verify data integrity [Weber (1986)]. Evaluating system controls involves determining whether controls exist and if they function properly or not.

Research indicates that CBIS auditors tend not to utilise sophisticated computing techniques to collect and analyse audit data. [Jancura et al (1983)]. While studying the effects of internal auditing techniques on external auditors, Rittenberg & Davis (1977) noted that the two internal audit activities most likely to affect the external auditor's work, viz., embedded audit routines in programming and the use of test-data. These were among the least used techniques encountered and that neither internal nor external auditors emphasised processing controls, which are the most technically complex set of controls and require additional technical training and experience [Weber (1980)].

One key issue in establishing the auditability of Computer systems is the maintenance of appropriate audit trails [Davis (1974); Kaunitz et al (1984); Menkus (1985); Wetherbe (1979)]. Audits trails can be used to review individual or groups of transactions and to track irregularities. In advanced computing environments that use on-line systems or other forms of communication, there is a trend toward elimination of printed records [Allen. (1960), Pathak, (1992)]. In



earlier generations, these records provide the basis for 'hard copy' audits trails. Now, in many cases, major application audits trails are only available in electronic form. To conduct audits in environments that have computerised audits trails, the auditors needs to use the computer itself as a tool in the audit process [Hansen et al, (1984); Wasserman, (1969); Pathak, (1988)]. Appropriate decision support systems (DSS) can be significant aid to auditor decision making in more advanced computer environments, those with networking technology, integrated data base applications, computer generated transactions, etc.. Examples of this kind of DSS are amply discussed in Davis et al (1980).

A typical problem with automated audits trails is the preponderance of data that must be reviewed. The same problem exist in analysing systems performance [Pathak, (1988)]. Performance reviews require an understanding of a system's work load and projections of current and future service level requirements [Kovach et al, (1984)].

In either case, too much data can be deterrent to effective auditing by obscuring the auditor's observation with information overload and unnecessary detail. Summarising and compacting automated audit data into a meaningful and usable format is an important part of utilising audit software efficiently [Kaunitz et al (1984); Davis et al (1980)].

Computing and networking systems are subject to threats from environmental disaster, mechanical failure, operator errors, programme errors, theft and fraud, and sabotage [Allen (1968)]. In order to be prepared to deal with such threats,

management must apply business discipline to its information systems environment Mc Farlan (1973) suggests that there are four key topics that management must continually question:

1. Management control;
2. Resource allocation;
3. Operations and technology management; and
4. Project management.

In practice, the CBIS auditor's role is to review each of these areas as they relate to specific systems environment and to diagnose current and potential problems in the environment [Pipino (1978)].

Ackoff (1978) defines control as 'the evaluation of decisions, including decisions to do nothing, once they have been implemented'. He describes that the process of control involves four major steps :

1. Predicting the outcomes of decisions in the form of performance measures;
2. Collecting information on actual performance;
3. Comparing actual with planned performance;
4. Correcting procedures based upon poor decisions, once identified, and correcting consequences as required.

Basically, auditing is evaluating the decisions of management objectively to assist management in improving its performance. The CBIS audit function evaluates an organization's use of computers [Nolan (1982)]. Additionally, the audit review process plays a central role in helping management learn about the opportunities and issues involved in effective utilisation of computer technology. This

learning, which tends to be focused on the audit committee's responsibility for reviewing the adequacy of internal accounting controls [Buss et al (1984)].

Review of the categories of key management topics are routinely conducted by CBIS auditors in several general areas. Three areas of interest are distinguished by Van Zutphen (1980) :

1. Audits of operational systems;
2. Audits of computer centers; and
3. Audits of systems under development.

Davis (1974) states that a management audit of the EDP or information systems function evaluates the following :

1. Adequacy of systems management;
2. Actual costs and performance compared to plan performance of existing applications; and
3. Adequacy of controls for protection of resources against error or loss.

A study conducted by Rittenberg & Davis (1977) yielded the following categories

1. Data processing management audits;
2. Data processing operations audits;
3. Design phase audits; and
4. Post-implementation audits.

These four categories of information systems audit activity are used as the classification structure for audit activities in the discussion that follows.

The audit related to data processing management focuses upon how well the management of the information systems function uses its resources to accomplish its objectives. Having a good statement of objectives and a long range plan is essential to this management function [Nolan (1982); Synott et al (1981)]. Procurement practices for costly data processing and telecommunications equipment, and any associated computer systems and network capacity planning strategies/methodologies, should be examined [Freed (1969)]. The capital budgeting for computer equipment, as one basis for procurement, also warrants careful evaluation. An unbiased professional review of the technically complex allocation decisions associated with computer equipment acquisition is an essential management audit function. Otherwise, management cannot avoid the situation in which the individual requesting the expenditure is the only person technically qualified to review the request [Gallinger (1980)].

The charge out mechanism, is used to charge expenses incurred to provide computer resources to the end-users of those resources. A review of charge out procedures is an integral part of CBIS audit. The charge out policy in use influences how resources are used, the direction and rate of technological change in the organisation, and the accountability felt by users for their own computer usage. Charge out policy is one indication of the overall strategic posture regarding the use of computer in the organisation [Davis et al (1980); Dearden et al (1973)].

Maintaining the adequate security is a major source of concern in data processing operations auditing. Valuable assets are frequently represented as information stored and manipulated in computers or traversing networks. Such intangible

property is becoming the object of attack in the increasingly computer-oriented environment for business, and for white collar crime [Parker et al (1984)]. The proliferation of the computer has increased the threats and risks, associated with criminal behaviour. Even one instance of automated fraud perpetrated with the leverage available using computer technology may lead to financial disaster. A single loss can be devastating [Parker (1979)].

Almost all the computer systems are vulnerable to physical destruction, data manipulation, theft of services, browsing, and the theft of targeted information [Perry et al (1984)]. These threats come from computer operators, programmes, authorised users, or unauthorised personnel. Perhaps, surprisingly, a study indicated that a higher level of competence in the computer programming staff was perceived by the management to increase the risk of exposure to unauthorised actions [Williams et al (1985)].

Internal data processing personnel conduct security audits of information systems facilities, giving the indepth reviews of both physical and data security [Buss et al (1984); Parker (1983); Perry (1985)]. Parker (1984) explains six functions into which information systems security can be structured :

1. Avoidance of loss by separation of assets and potential threats.
2. Deterrence by stopping personnel from positioning themselves to engage in unauthorised activity.
3. Prevention by configuring the systems to block the unauthorised acts.
4. Design of adequate recovery capability in systems to minimize harms after loss.

5. Timely detection of losses, or impending losses, to stop or minimize any exposures that result.
6. Correction of weakness and associated vulnerability so risk of loss is reduced.

Security audit involves reviewing each of these areas. The CBIS auditor may be involved in reviewing any of these areas too, depending upon the requirements of a particular audit engagement. The primary focus of the auditor includes the last two items, the timely detection of losses or potential losses, and the correction of weaknesses and associated vulnerabilities [Porter et al (1984)].

The CBIS auditor's participation in the design of applications systems during applications development projects is referred as design phase audit. It is the auditor's primary responsibility in these projects to ensure that computer systems are auditable when they become operational [Wasserman (1969)]. The auditor is concerned with the adequacy of control structures in the design phase (of the typical life-cycle methodology for application systems development) and the effectiveness of resulting controls during the testing phase [Weiss (1980)]. In a study, Helms (1983) found that auditor involvement in systems development projects positively affected the quality of the systems developed. These included user satisfaction, subsequent system maintenance, and budget variances.

It was further suggested in yet another study that there should be an approach to monitoring a system throughout its useful life and that monitoring should be done by the CBIS auditor [Lientz et al (1980)]. Audits of existing systems including post-implementation audits are vehicles for accomplishing this objective. The focus of these audits is the systems maintenance process. Implicit within the

CBIS auditor involvement in system development projects, is the assumption that such involvement will reduce maintenance costs over the life of the system [Helms et al (1983)]. During audits of existing systems, the auditor focuses upon the basic maintenance functions for each systems, as well as problem identification, tracking and resolution procedures and change control procedures for system modifications [Bradley (1985)]. As Swanson (1976) indicates, there are three categories of systems maintenance :

1. **Corrective maintenance** performed in response to assessment of failures;
2. **Adaptive maintenance** performed in anticipation of change; and
3. **Perfective maintenance** performed to eliminate inefficiencies or to enhance performance.

During the audit of the existing systems or the post- implementation audit, an auditor diagnoses problems with (or related to ) the system under review in each of these areas and recommends relatively minor improvements or, perhaps, major system enhancements, as appropriate [Weber (1984)].

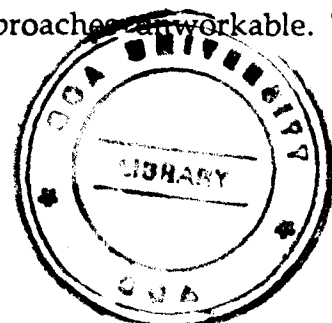
Most of the existing systems installed in computer facilities are not internally developed, but are acquired from outside hardware and/or software vendors. Auditors examine these systems for evidence that the vendor has included sufficient data integrity and programme reliability controls into the systems and that these controls are properly installed and functioning [Perry (1984)]. Particularly. If the systems are complex they should also provide mechanism (such as standardised programmes and software tool) that aid the reviewer in the examination and verification of system processing accuracy and reliability [Menkus (1985); Wasserman (1969)].

In nutshell, the principles of CBIS auditing deal with general theories of auditing and with audit techniques. These principles also deal with the content of audits by identifying several candidate targets for a CBIS audit. These include organisational targets (such as data center management, computer operations, or applications systems during design or post-implementation phases), and functional targets (such as systems charge control or data security). These principles can, and do apply equally well across technologies. Obviously, these principles deal with what to do, not how to do it. There is considerable room for judgement.

Auditing of computer installation is very different from auditing in terms of how to do it effectively. Thus, in specific circumstances, it is the professional judgement of the auditor when assessing the situation that controls the content, and ultimately the effectiveness, of a given audit.

### **Factors Affecting Auditor's Judgement**

The major contributor to CBIS auditing success or failure is the professional judgement of individual auditors. The objectives and general characteristics of accounting control do not change with the method of data-processing utilised in an organisation [AICPA (1978)]. Therefore, it has been possible to develop general guidelines for CBIS auditing that correspond to the various categories and techniques described previously [Harper et al (1982); Litecky et al (1981)]. However, none of these can be precisely defined as to its specific content for specific situation. The variety of technologies and implementation strategies possible, and the instability introduced into organisations by changing information technologies make inflexible auditing approaches unworkable. The CBIS





auditor must ultimately rely upon individual judgement in determining the specific content of a particular audit engagement. Therefore, the auditor must consider the unique characteristics of each individual situation and plan that engagement accordingly [Holley et al (1983); Litecky et al (1981)].

Objectivity is the most important factor influencing the CBIS auditor's judgement in an audit. One, and perhaps the most generally accepted, approach to ensuring objectivity of the auditor is to maintain a high degree of independence between auditor and auditees [Lathorp (1985)]. Such independence should be maintained and clearly exhibited when reporting the audit results to management. Independence between the auditor and auditee is a professional need for audit effectiveness regardless of the financial, organisational or technical factors that, along with auditor judgement, determine the specific content of an audit engagement [Parker (1981)].

The levels of audit testing and the auditor's evaluations of internal controls are based upon the auditor's judgements [Joyce (1976); Mason (1975)]. There are no objective measures to evaluate the relative quality of different auditing decisions [Joyce et al (1982)]. The adequacy of controls and levels of compliance and other testing that may be needed during an audit depend upon subjective interpretations of complicated situations. Therefore, auditors have adopted a consensus seeking posture in audit engagements [Weber (1980)]. In effect, 'generally accepted principles of CBIS auditing' are agreed upon and maintained by the profession as the standard against which to make technical judgements [Deloitte et al (1983); EDPAFER (1980)]. Thus, it becomes reasonable to argue that 'any professional CBIS auditor' would arrive at essentially the same conclusions in a

particular engagement [Trotman et al (1985)].

The comparison of management techniques and controls in multiple organisations is another important audit technique that strengthens the consensus seeking paradigm [Perry (1985)]. Comparative analysis establishes base lines for levels of system-related controls across organisations of approximately the same size, or in the same industry, etc. A study in USA (in manufacturing sector) found that the larger the company, the greater the likelihood that management would regularly require auditing of its computer work [Dean (1968)]. Such information provides a general frame of reference that may be useful in evaluating other manufacturing organisations in the future.

On the issue of conflict resolution between auditors and clients, it was found that auditors stressed achieving consensus on technical matters while clients stressed effective performance [Monger (1981)]. Another similar type study indicated that data processing personnel place emphasis upon establishing controls through applications of technology while audit personnel put emphasis on controls that are based upon obtaining approval from appropriate authorities [Norris (1983)]. Both the studies depict the auditor's disposition to deal with complex technological issues by using consensus building and reliance upon professional judgement as surrogates for detailed technical understanding of specific applications of information systems technology. Obviously, as the complexity of such applications of information technology increase, reliance upon consensus building in information systems auditing must give way to increase technical specialisation among CBIS auditors.

The review of literature covering the various information systems auditing topics that are needed in order to address the auditability of computer networks is complete by this last section on auditor judgement. While many of the concepts and issues related to auditing networking (both LAN & WAN) are essentially the same as those that apply in other form of CBIS audit, even then there are substantive differences. These are examined below.

### **Computer Network Auditability**

With the greater sharing of data by user and more use of distributed computing and teleprocessing systems the computer communications controls are becoming increasingly important [Martin (1981 a); Synott et al (1981)]. As a direct result of these trends, the importance of computer communications controls in information systems auditing is expanding accordingly. Such dramatic communications network growth is not without its problems. Control techniques for computer networks are still unsophisticated by comparison with the controls that are now commonly used with main frames, and even smaller computers [Bailey et al (1982); Davis et al (1983 a)].

Data telecommunications audit involves four steps :

1. Identify expenses;
2. Review contracts;
3. Establish equipment logs; and
4. Identify potential cost savings.

In comparison to CBIS auditing described in earlier sections technology auditing is very limited concept. The focus of this process is eliminating waste, and not

safeguarding assets, and illustrates a general lack of conceptual clarity in this arena.

There is the inter-relationship between audit requirements & control processes which reflect in the concept of auditability [Perry et al (1978)]. The control of complex network systems involves all of the basic control mechanisms that are utilised in computer systems controls [Frigon (1983)]. The architecture of networks, because of the geographic dispersion of their component parts, raises complex new control issues which are not common in conventional computer installations [Parker et al (1984)]. Furthermore, the current expansion of network capabilities and traffic volumes threatens to outpace the development of counter-vailing network controls [Diebold (1985); Folger et al (1983)]. As Anthony (1965) has stated the 'information handling specialist' has a dynamic responsibility to utilise new techniques for the improvement of the information used in management control and operational control processes. Network control systems are among the newer techniques for information handling that will have major impact upon future CBIS auditing practices [Holley et al (1983); Pocek (1985)]. What this means for network control strategy is that because the information system network in advanced applications is at the center of information handling activities, the control strategy for the network will be central to the computer-based information systems audit process. Network control is not only important for network management, but also enhance overall information systems control capabilities.

The primary issues in general management network control are asset safeguarding, data integrity, system effectiveness, and system efficiency [Weber (1984)].

These are the same issues that are key in administering computer systems control [Vanecek et al (1983)]. In the network environment, the implementation of controls has generally focused upon the following [Weber (1984)] :

1. Error detection on a line;
2. Treatment of line errors;
3. Choice of network topology;
4. Choice of network equipment;
5. Choice of communications medium; and
6. Use of Cryptography.

These are the network design criteria that must be evaluated in order to implement a network and not controls in the sense of establishing auditability. Certainly controls can be established that relate to each of these areas in a specific network. Nevertheless, such measures alone do not provide a practical structure for determining the extent to which the network facilities help in achieving management's information system objectives [Ghosh (1989); De Witt (1992); Stewart (1979)].

The objectives of information systems for network management can be summarised as follows [Menkus (1983)] :

1. Deliver a message fully and accurately to its intended destination and nowhere else;
2. Protect the contents of that message, whether wholly or in part, by not disclosing except to the intended recipient;
3. Avoid (or survive) operational failure due to natural or man-made disasters; and
4. Offer a high degree of consistency and reliability.

Considering the complexity of technology alone these objectives are difficult enough to achieve [Deen et al (1988); Burns et al 1992); Carol & James (1992); Perkins (1983)]. The growth in the use of the technology and the underlying technology itself are evolving rapidly which has become a serious problem for the auditor. New exposures are being created and old exposures are gaining in materiality within an audit. The network environments are fast becoming vulnerable from hackers, professional criminals and unscrupulous employees. Computer networks are under attack and, through them, information systems are becoming more vulnerable. Network integrity is too often and too successfully being compromised both actively and passively, as follows [Carol & James (1992); Chaffee (1987); Parker et al (1984); Reel et al (1985); Ware (1984)]:

1. A passive attack is one that causes an unauthorised release of information;
2. An active attack is one that causes either unauthorised modification of information or unauthorised denial of resource use.

Such kind of attacks can be either deliberate or inadvertent. In either case, the control mechanisms for the computer network are compromised [Allen (1968); Carlson (1982)]. The information systems auditor's contribution to network management must be to assure, within the bounds of materiality, that the telecommunications network in use in an organisation is not only tamper-proof but also error-resistant, so that information that is transmitted is received correctly; in other words, that messages communicated over the network are kept both accurate and secure [Communications Int. (1987); Chakraborty et al (1990); Holley et al (1984)].

Networks are subject to security violations at any node or along any link, and such links, called 'lines', can be via microwave, land lines, radiowave, satellite, or fiber optic media [Communications Systems Worldwide (1988); Synott et al (1981); Tanenbaun (1981); Davis et al (1979)]. These point to point links conform to a given topological structure or 'physical distribution' [Baker (1980)]. Many of these links are provided by common carrier telephone lines, but most insecure medium of communication. These lines were actually designed to carry voice messages between the nodes with reasonable accuracy. At that time, hardly ever a thought was given to protecting the content of those messages against compromise or manipulation [Grehan (1990); Menkus (1982)].

There are two basic approaches to achieve the security in network communication [Haldar & Subramanian (1989); Voydock et al (1983)]. The first approach is 'link oriented' that provides security by protecting traffic independently on individual communications link. The second approach includes 'end to end' technique that provides uniform protection for each message from its source to its destination. Depending upon the topology of the network involved either of these may be appropriate manipulation [Harman James (1987); Menkus (1982)].

Choosing the appropriate set of controls is a complex and involved process. Many potential controls are too stringent for practical applications. The number and type of controls must be based upon the sensitivity and criticality of the information being used [Wood (1984)]. The commonly recognised procedures that can be used to control security within telecommunications networks include the following [Fritchman (1984) Hirschhein & Newman (1988)] :

1. Software control for network access (codes such as passwords or user's IDs;
2. Physical locks on terminals;
3. Physical terminal identification;
4. User and terminal programme identification;
5. Network sub-system access control;
6. Encryption procedures; and
7. Packet Switching.

The extent to which computer networking is vulnerable to a wide variety of control violations and the extent to which networking management needs effective auditing is shown in a study [Guynes et al (1983) Hull et al (1991); Igarria et al (1991)].

Policy reviews are an important part of the management audit process [Davis (1974)]. Within the discipline of telecommunication there are two theoretical schools of thought [Burg et al (1984); Institution of Engineers (1989); Jaikumar & Gomez (1986)]. One view holds that the function of a network is limited to moving bits from one end-point on a network to the another [Mathias (1982)]. In other words the network should never contain any logic with which to examine the semantic content of messages transported, except as content related to the transport function it-self. Accordingly, the network is considered inherently unreliable and the process of recovering from errors should reside with the terminating systems. The second philosophy of networking endorses added functionality within the network and not in the terminating systems.



Functionality can be added to a network in three ways [Frigon (1983)] :

1. The mainstream concept, promoted primarily by the mainframe computer manufacturers, integrates the network management function in to various networking computers;
2. The sidestream method of network control, advanced primarily by modern manufacturers, uses a secondary channel to communicate with various intelligent network parts;
3. The overlay technique is vendor independent and consists of probes and "black boxes" that are installed between adjacent network elements.

Individually these techniques are being pursued by vendors of telecommunication equipment. These are being implemented in organisations and their integration into complex computing and networking environments is increasing the overall technical complexity of information systems environments. The information system auditor must assimilate this new complexity [AICPA (1978); Davis et al (1983b) Packer (1981)]. New techniques and new tools are needed to support the auditor in the review and evaluation process [Bailey et al (1982); Spooner (1987)]. Telecommunications applications create situations in which the CBIS auditor is required to audit with the computer as well as through it [Holley et al (1983); Read (1989)].

The most important tools used in network management are configuration control, status management and diagnostic support [Raymond (1987); Seid (1983)]. New automated methods of monitoring, trouble shooting and measuring performance of data communications lines are being implemented in corporate networks [Weber (1984)]. These new facilities will be an invaluable help to the

information systems auditor. One method, called intelligent monitoring, includes analysis and reporting of line traffic, error alarms, and network diagnostics [Pearson (1989); Pocek (1985)]. All of these functions operate on a multiprocessor-based network analyser, that is a separate computer that passively monitors network activity and records summary statistics and unusual events.

The new tools will eventually lead to meaningful comparative measure between similar types of network applications [Garrison (1984); Salsburg (1984) Walko (1988b)]. One of the early attempts to develop "a capacity index of network efficiency" appears interesting for some limited but important circumstances [Johnson (1985)]. Because of the judgement nature of auditing, these kinds of comparative indices will be valuable in auditing network facilities [Wabler (1984); Woodburn (1987)].

The objective of audit trails, in networks as with individual computers, allows the reconstruction of actions and interventions those have affected systems' components and states over a given interval of time. Audit trails are needed to record the source, and occasionally the entire route, of a transaction as it travels through a network. Ideally, each node, port and terminal in the network that a message passes should be identified as an appendage to the message and the message time stamped at each point [Fidlow (1985); Van Name et al (1990b)].

With appropriate naming conventions for transactions and table-driven applications software to report on transaction traffic, useful workload profiles can be constructed [Davis et al (1980)].

These kinds of profile are typically used to develop network design criteria and can be useful to the auditor in establishing audit requirements during planning of a network audit. Five basic profiles are used to define network design criteria [Levin (1984)] :

1. User profiles (by functional area and location);
2. Usage profiles (Availability, peak loads, etc);
3. Geographic profiles (User population density etc);
- 4 Application profiles (transaction mix, response times, organisational impact, etc);
5. Hardware profiles (device needed where and by whom).

The basis for periodic status reporting is provided by each of these operating profiles. One of the primary purposes of network status reporting is to identify major trends, such as increasing traffic in part of the network and any related response time degradation, which may indicate the approach of thresholds that affect network performance significantly [Elkins (1985) Van Name (1990a)]. Such information is basic to the network auditor who is charged with reviewing management's networking decisions [Davis et al (1983)].

It is necessary to give reasonable assurance that a new network component, once installed, will perform as desired and that it will not degrade the other components of the network [Salsburg (1984); Thomas (1992)]. The auditor can forecast work load and predict resulting response times, for all network components under a reasonable set of alternative traffic Scenarios. It is also useful to determine which components of the network will become bottlenecks as the work load changes, so that management can plan computing and network resource

acquisitions accordingly [Stewart (1979)].

In summary, modern complex computer networks environment are difficult to manage and , therefore, difficult to audit. Network controls are not well established to begin with and dramatic increases both in the amount of networking services being implemented by organisations, are increasing exposures. Because network control is surfacing as an integral component information systems control strategies, increasing exposures in networks have the potential to undermine general information systems auditing objectives.

At the same time, managers have an ongoing responsibility to improve information handling to enhance management and operational control. New tools and new standardised measures are needed; better audit trails too are essential. The potential for improvements in network intelligence cited above will provide managers with new, significantly improved tools for approaching this responsibility.

Furthermore, the increasing complexity of computer communications will dictate an intelligent networking approach to enhance the network control. More effective usage reporting and work load management techniques are necessary as a basis for networking planning and to establish useful baselines for implementation of control strategies.

The growing importance of computer networking in information systems is increasing the materiality of network controls in audits. Simultaneously, increasing complexity of networks is rendering them more difficult to audit under the

traditional CBIS auditing paradigms. If these trends continue, a situation could arise in which complex computer networks essentially cannot be audited effectively.

Consequently, a shift in the computer based information systems auditing paradigms is in order to adapt the auditing process to the new realities regarding the operational impact of computer communications technologies upon business organisations in the 1980's and 1990's.

In the next chapter of this doctoral thesis, a theoretical model of information systems auditing will be presented that addresses the issue of shifting paradigms. This model will serve as a basis for the development of the research design employed in this research effort.

## **CHAPTER 3**

### **THEORETICAL FOUNDATIONS**

Though there had been a considerable quantity of theoretical work in the area of computer based information systems (or CBIS) and its various aspects as explained in the previous chapter on review of literature which collectively provided the important conceptual insights, this theoretical work has not added substantially to the empirically-based studies in this field. Very few of the studies conducted so far dealing with the systematic and controlled research environment have found place in the review. Particularly, far and few researches have been observed in the area of auditing telecommunication network-based distributed data processing.

Very few studies reviewed in the earlier chapter were concerning computer based information systems auditing and included atleast some portion of distributed data processing and network environment evaluation. One of the studies found the audit implications of distributed data-processing by conducting the survey of 161 auditors with an average 9 years of experience [Lamp et al (1984)]. It was found in their study that new or enhanced exposures that resulted from implementation of distributed systems architecture were perceived by the auditors as having 'strong' or 'profound' disruptive effects on traditional internal controls.

This chapter begins with the introductory section on the overall structure of this research study. In all, it consists of nine parts, and the introductory section is

succeeded by a section dealing with the information systems audit-cycles and provides a theoretical framework within which to position the current research effort. A review of the concept of critical success factors and its application to questions of audit effectiveness is included in the third section. Rest of the section addresses a control objective of this chapter. With its focus on the theoretical foundations supporting this research, this objective is to develop a general conceptual model for information systems audit engagement planning. This model addresses the definition of audit requirements, the preparation of plans for resource allocation, and the selection of appropriate procedures for use in the audit. The model is applicable to a wide range of CBIS auditing situations and helps to provide an appropriate basis for subsequent systematic research.

General information systems(IS) auditing framework, including both manual and automated systems are discussed in the beginning of this chapter. Then, the focus narrows from the consideration of computer-based information systems, including both computing and networking technologies used in distributed data processing in corporate sector.

### **O v e r a l l   R e s e a r c h   P a r a d i g m**

The role of networking technology in information systems is growing dramatically, as has been seen in Chapter 1 and Chapter 2. This growth is not only changing the nature of information systems in organisation, it has become reasonable to expect that a corresponding effect on the CBIS audit function is also growing. This research effort is primarily interested in the identification and comparison of specific key factors in audit engagement planning that contribute

to the success/failure of CBIS audit engagements in two distinct scenarios (i.e. technological environment). A documentation of important differences in CBIS auditing practices is expected in this analysis of two sets of factors in two environments.

The first scenario is the computing environment with least networking and mostly centralised and traditional in outlook. It includes the hardware and operating software, application software, technical personnel who operate and maintain the system environment, and the procedures and methodologies, used to organise and execute job-assignments. All of these are basically computer oriented components of the information systems environment taken from a wholistic information handling perspective.

The second scenario is characterised by a significant networking component that supplements the computing component of the information systems technology architecture. This second scenario includes both computing and networking components, which translates into two kinds of hardware and operating software systems, two kinds of technical personnel to operate and maintain the systems environment, and often two sets of procedures to organise and execute work tasks.

The technical characteristics of the two scenarios mentioned and the implications on CBIS auditing are of interest in this research. Also, the various relationships between the computing and networking systems audit components within the more advanced environment is an important focus for this study. Throughout



this research, the first category of systems is referred to as the 'Traditional' information systems technology and the second is referred to as the 'Advanced' information systems technology.

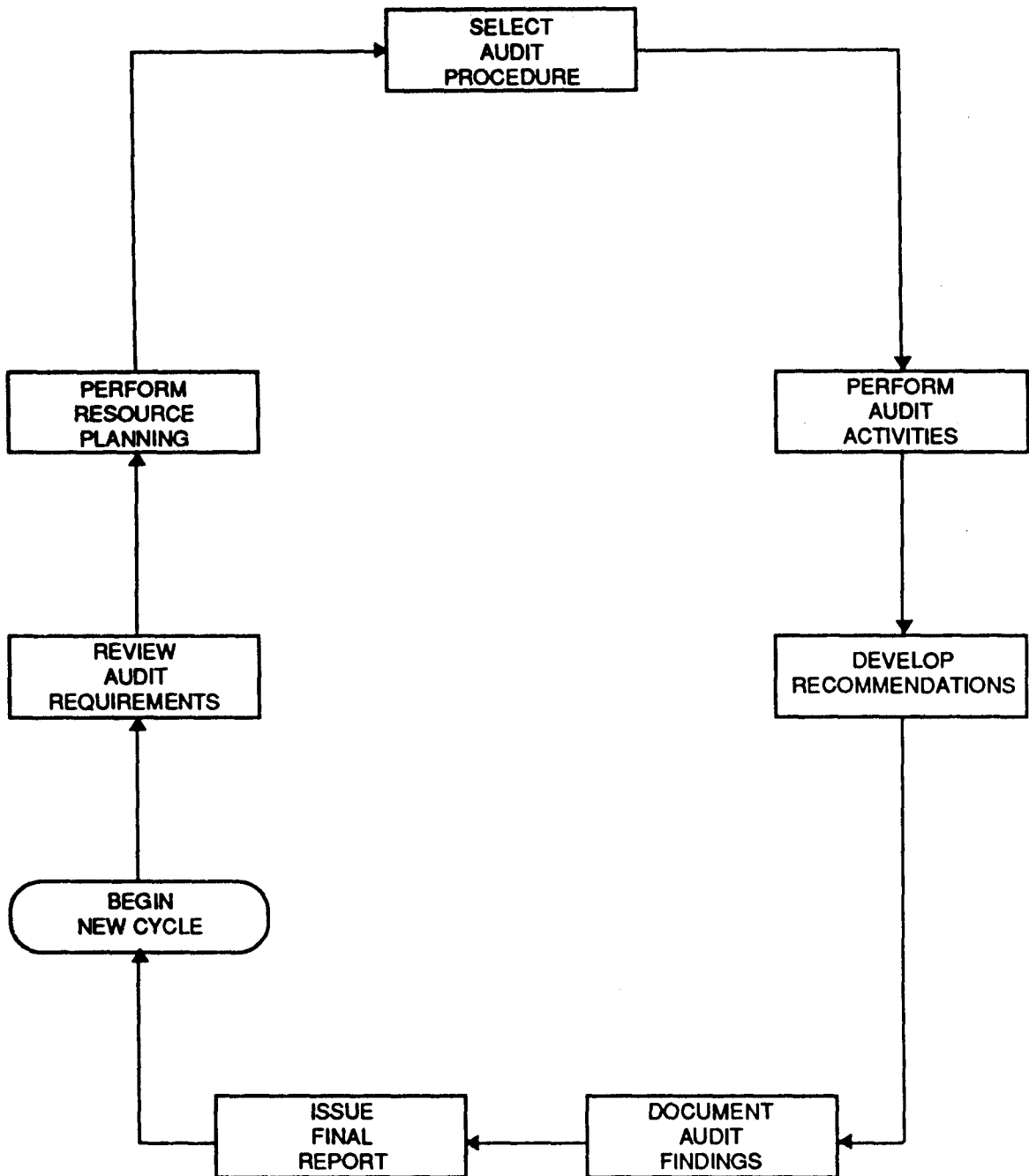
## **A u d i t C y c l e s**

Audit cycle in information systems focuses on the periodic evaluation of an organisation's use of information technology. A series of routine steps, cyclical in nature is included in the audit process. These are shown in Figure 3.1.

Every audit begins with an appropriate assessment of current audit requirements including a review of the status of previous audits, the development of a plan for the allocation and utilisation of resources during the audit, and the identification and selection of a set of audit procedures for use during the audit. The CBIS auditor then conducts the CBIS audit portion of the audit, develops appropriate recommendations, fully documents the findings, and issues an appropriate report.

The documentation of the CBIS audit is filed and is made available during subsequent periods as background information for use in preparing for the next audit, which begins a new audit cycle. Generally, the efforts of the audit between successive audits and in response to the CBIS auditor's recommendations are documented and filed with the audit archives in order to maintain thorough and complete records for use in future CBIS auditing cycles. Particularly in dynamic environments, the content of each CBIS audit engagement evolves over time to adapt to changing circumstances in the organisation. This tends to be the case for

**Figure 3.1**



**AN AUDIT CYCLE**

any type of audit, irrespective of internal or external, manual or computer-based systems. Regarding CBIS auditing, the changing technology and the variety of new system implementations typical of modern business organisations often ensure that the information systems environment remains dynamic and, therefore, the content of each successive audit cycle is different. That difference encompasses more than the closed loop represented in Figure 3.1. This is because an audit consists of both content and structure, and Figure 3.1 deals only with structure.

External factors, such as adaptation of new systems technology, can significantly influence the content of successive audit cycles. When changing information systems technology is considered, the CBIS audit cycle can be thought of as an 'audit spiral'. Each successive audit can be considered to progress along a hypothetical new scale of increasing technological complexity. Various factors that influence the success of CBIS auditing engagement are at least partially, determined by the extent to which the auditing spiral can be made to correspond with the evolutionary progression of information technology within the organisation being audited.

### **Critical Success Factors**

The concept of critical success factors (CSFs) as a technique is to assist managers to direct their energies toward those activities that increase their managerial effectiveness [Rockart (1978)]. Different situations may have different critical success factors for different managers. Similarly, CBIS auditors can utilise CSF types of evaluations in determining the effectiveness of audit engagements.

Because auditing itself derives from the delegation of a portion of the control function of general management. It is possible to make a reasonable and parallel application of Rockart's research on CSFs for business executives to the functions performed during the CBIS audit cycle. Four methods of determining executive information requirements were described collectively in the researches conducted by Rockart (1978) and Mintzberg (1976). These four methods are as follows :

1. By-Product Method :- The data generated are used being a by-product in the normal process of computerisation of operational systems, without any regard for information requirements.
2. Null Approach :- This method shuns computer based information as unimportant. Because, this approach is based upon the premise that management is a dynamic process, that is future oriented, subjective and based upon informal information that is mainly word-of-mouth.
3. Key Indicator Method :- This method is acquiring favour rapidly among the CBIS auditors community. It is based upon three types of factors including overall business indicators, 'exception' indicators and better computerised presentation capabilities for displaying indicators.
4. Total Study Method :- This approach is cumbersome to maintain, inflexible, and expensive. It is based upon formal methodologies in which the overall information requirements of management are received and structured into systems development requirements that supplement the By-Product Method.

These approaches correspond to information environments those are typical of various individual situations in which auditors must conduct reviews of information technology usage. Just as with the general management function, the

information required by CBIS auditor includes an inherent need for data organisation and focus that builds upon and goes beyond these earlier methods. Critical success factors provide such an approach. Without a technique such as CSFs for CBIS audit engagement planning, execution, and evaluation, the CBIS audit process must be based upon techniques similar to those described above.

The critical success factors as a concept was originally discussed in the management literature by Daniel (1961) and expanded first by Rockart (1978 & 1979). One primary conceptual foundation upon which this research is based is the principle that critical success factors are well suited for determining the effectiveness of CBIS auditing activities.

The limited number of measures and judgements with which the auditor can assure the success of an auditing engagement are critical success factors in a particular business situation. In unison, these factors can be regarded as reasonably sufficient conditions for success. An appropriate set of critical success factors can be identified for each specific auditing situation. By classifying similar situations based upon general characteristics, such as levels of networking complexity involved, the critical success factors for CBIS auditing projects can be analysed by those classifications. Attention to those factors by the auditors during CBIS auditing cycles can then be expected to increase the effectiveness of the CBIS audits performed.

### **Audit Engagement Planning Process : General Model**

The main and the central focus of this research is to determine the critical success factors that practicing CBIS auditors consider as key during the process of plan-

ning for CBIS audits in both traditional and advanced information technology environments. The process of planning CBIS audit engagements includes the audit resource planning activities which are the primary focus of this research. Therefore, it is useful to first develop a general model for audit engagement planning. This theoretical model can be used to clarify the general concept of audit resource planning as well as helps to subsequently establish a research model to serve as the basis for this research.

Building upon the preceding descriptions of the CBIS audit cycles, the CBIS audit engagement can be decomposed into four steps, or echelons of activity, as follows :

- 1. Review Audit Requirements :-** The requirements definition is the portion of the audit cycle during which the environment and the existing situation is assessed.
- 2. Plan Audit Engagement :-** The resource planning activity is the part of the audit cycle during which the audit content, the specific areas of activity to be evaluated, are identified.
- 3. Determine Audit Procedures :-** The procedures selection part of the audit cycles involves choosing appropriate procedures by which to achieve the planned audit content.
- 4. Complete The Audit Cycle :-** The execution of the rest of the audit cycle involves performing the audit by performing the steps shown in Figure 3.1.

The first three steps of the audit cycle, which are the first three 'echelons' described above, comprise the process of audit engagement planning. These three steps are expanded into the theoretical model presented in this section of the thesis. It is important to note that each of the four echelons listed is inherently iterative in character. Information gathered at one echelon may influence decisions made previously, thus causing revisions of prior assumptions and strategies as the CBIS audit develops. Especially, in complex information systems environments, this iterative approach is characteristic of the process of auditing information system. Furthermore, it can be expected that each echelon will include certain critical success factors for conducting particular kind of audit engagements. Figure 3.2 depicts the structure of this process.

### **C o n t r o l   C o m p l e x i t i e s**

When an auditor first evaluates a specific situation, a collection of controls will have to be established that were previously deemed appropriate by management. These controls may be manual or automated, and may range from relatively simple to complex. Figure 3.3 illustrates these concepts in the form of an information systems control grids. The four quadrants of the grid can be classified based upon the computing and/or networking technical sophistication required of the auditor :

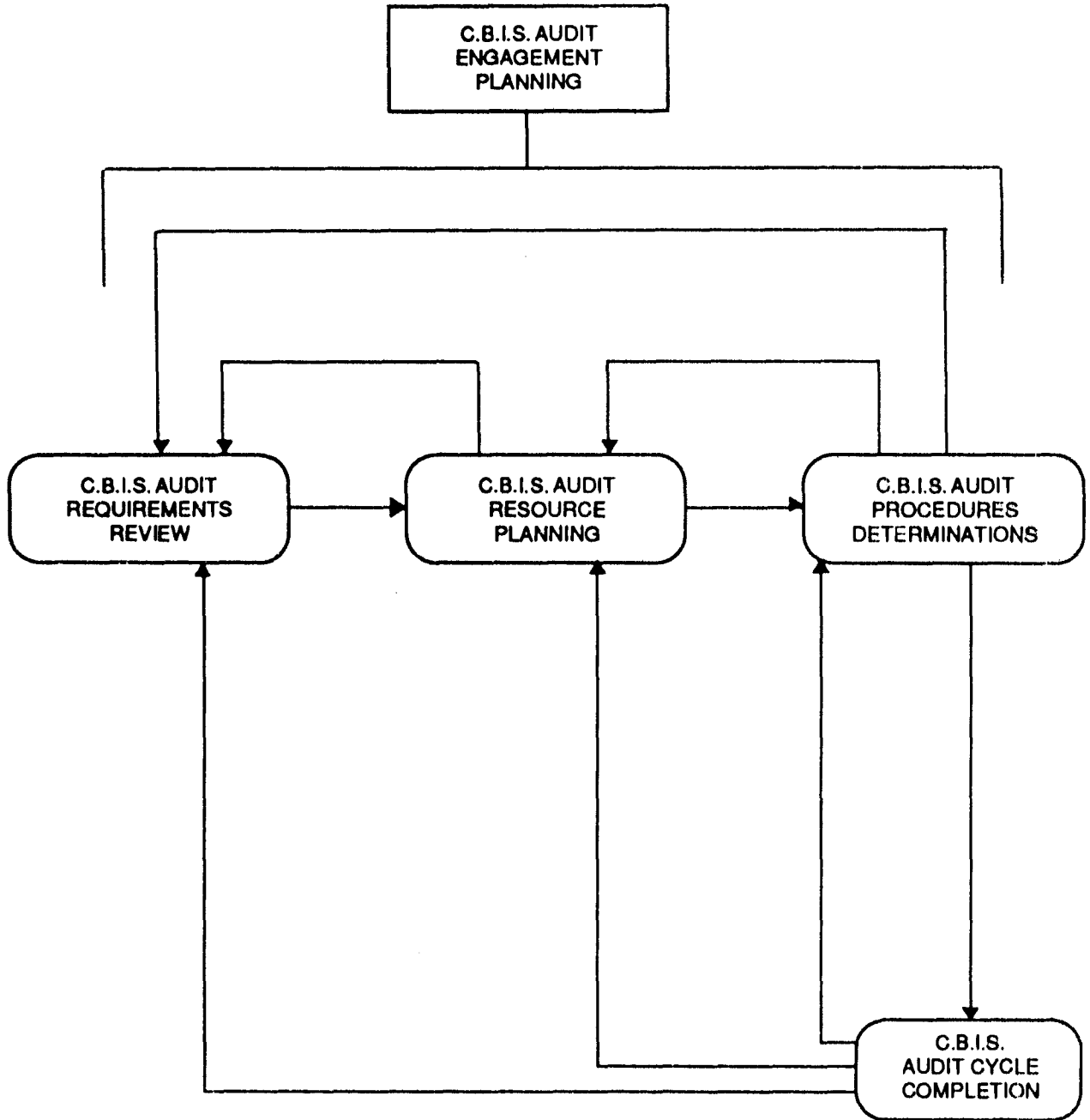
Level I - Simple manual control;

Level II - Complex manual controls;

Level III - Simple automated controls;

Level IV - Complex automated controls.

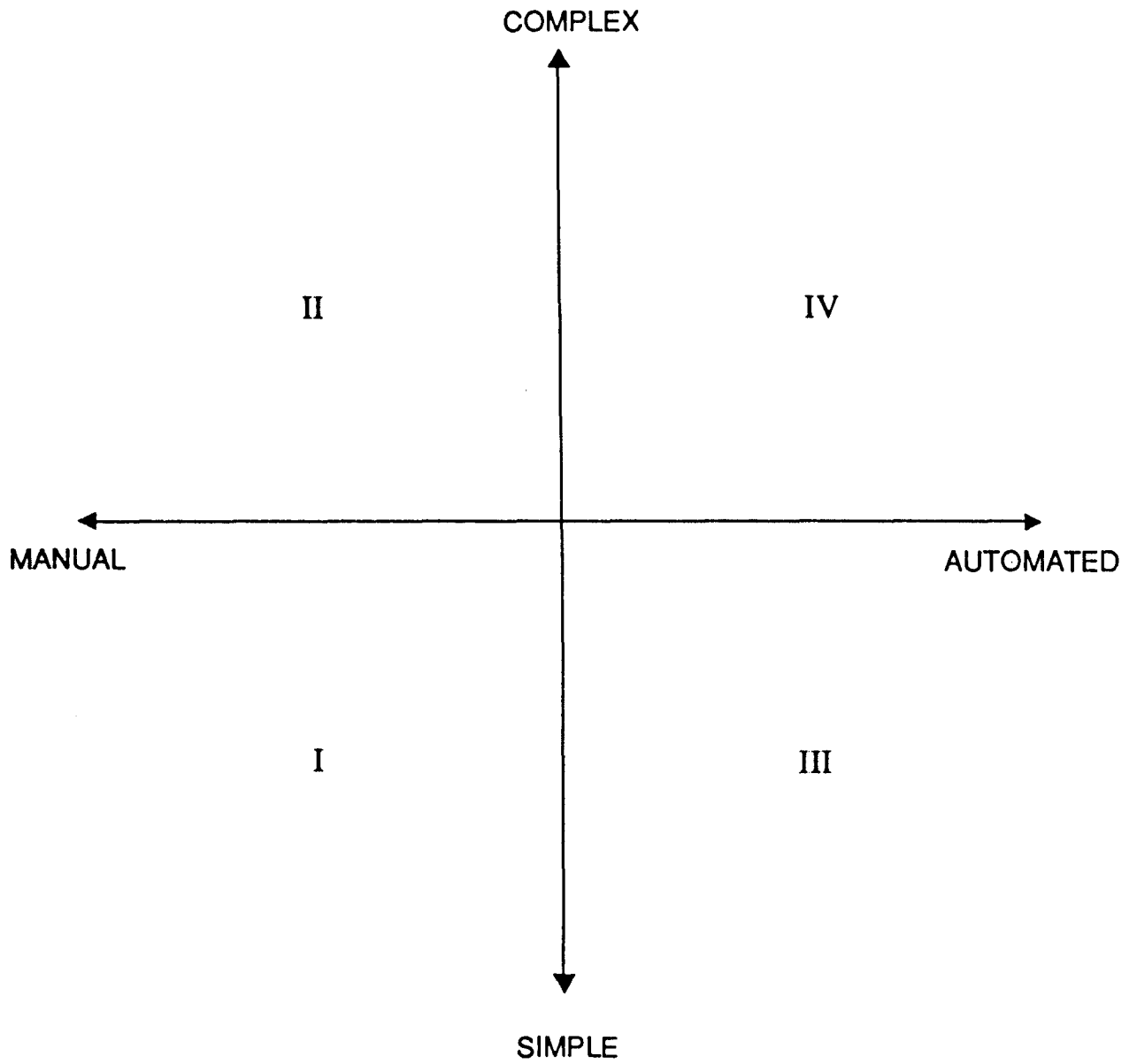
**Figure 3.2**



**PLANNING ECHELONS FOR C.B.I.S. AUDIT ENGAGEMENTS**



**Figure 3.3**



INFORMATION SYSTEM CONTROLS GRID

It is reasonable to expect that an auditor who is prepared and technically competent to perform audits upon a given level can effectively perform audits at any lower levels, but not at higher levels.

This research focuses on CBIS auditing in level III and level IV situations. The simpler automated controls tend to be associated with traditional batch oriented processing systems while complex controls tend to be associated with distributed processing environments. Unfortunately, complex automated (Level IV) controls are not widely implemented, or even well understood, yet [Weber (1980 & 1984); Wood (1984)]. Nevertheless, a systematic migration of CBIS audits into the Level IV category continue to increase in technical complexity into the future.

## **Theoretical Model**

### **Part I**

#### **CBIS Audit Requirements**

The first part of the theoretical model deals with establishing general CBIS audit requirements. Audit requirements can be thought of as absolutes. They exist in an abstract sense as a property of the business situation that is being considered. They are absolute at a point in time but not fixed over any specific duration. They evolve as technology changes, standards change, and organisations change. The penultimate objective of a successful CBIS auditor is to discover and address these changing audit requirements during each CBIS audit cycle.

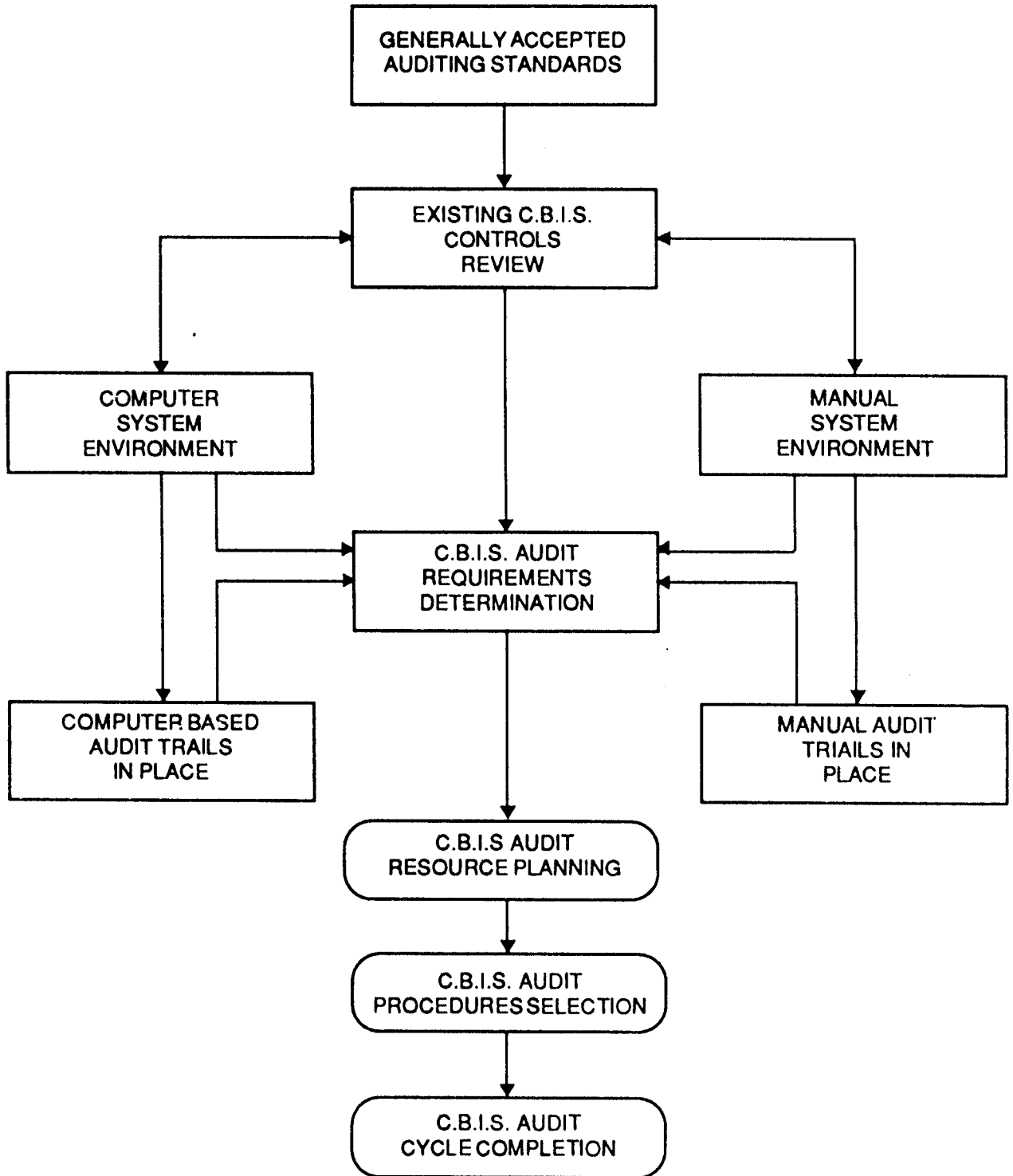
Considering a given organisation and period of time, CBIS audit requirements are related to the controls already in place and the manual and automated infor-

mation systems environments in use. The application of auditing standards to the evaluation of systems and controls in the previous CBIS audits generally affects the computer-based information systems controls that are in place. They help to highlight those areas needing improvement and, therefore, provide a steady pressure for positive change. Also the organisational environment, including both the manual systems and automated systems used, influences the CBIS audit requirements and the various controls that are established. Figure 3.4 shows these relationships.

This figure deals primarily with computer system component of CBIS auditing requirements. As the use of advanced tele-communications systems becomes more common place, a new component of CBIS audit requirements analysis is taken into account. The structure of a model of network audit requirements parallels the structure of computer audit requirements depicted in Figure 3.4. Thus, there is a duality in the structure of a complete model of the computer-based information systems auditing requirements analysis process, as shown in Figure 3.5.

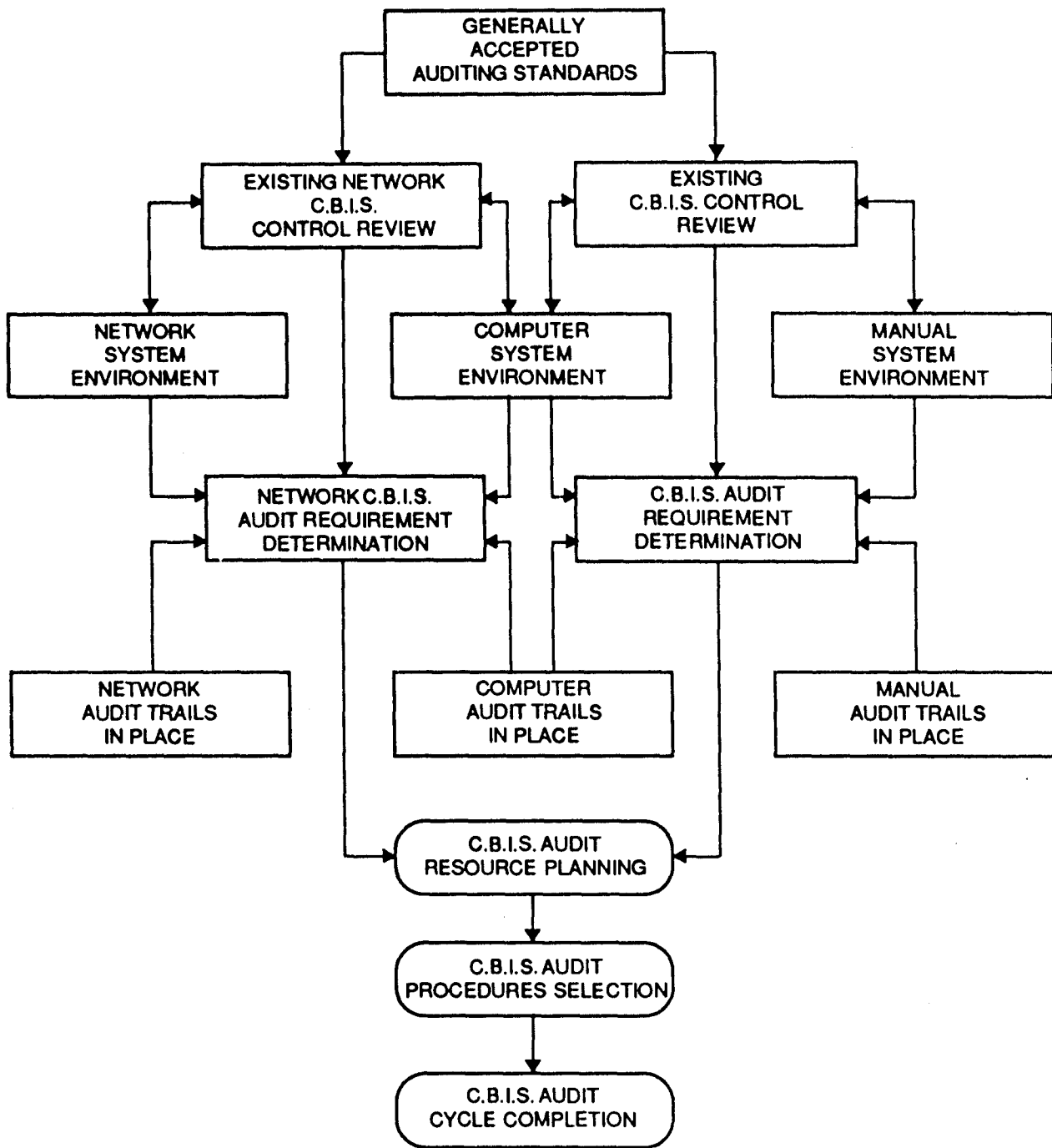
It should be noted that the auditor can consider that there is a continuum representing increasing information systems technical complexity moving from right to left across Figure 3.5. There are, of course, other factors that relate to increasing technological complexity other than networking; data-base architecture is an obvious example. These other factors are outside the scope of the current research.

**Figure 3.4**



DEVELOPING C.B.I.S. AUDIT REQUIREMENTS - (COMPUTER)

**Figure 3.5**



DEVELOPING C.B.I.S. AUDIT REQUIREMENTS - (NETWORK)

## **Part II**

### **C B I S A u d i t R e s o u r c e A l l o c a t i o n**

Once the CBIS audit requirements related to computing and networking have been specified, the planning of audit resource allocation that meet those requirements begins. The key here is the development of an appropriate plan for each cycle of the CBIS audit and the modeling of the factors that contribute to that development. This planning provides the link in the model between the definition of requirements and the determination of the content of the CBIS audit in terms of the specific activities to be addressed in a particular CBIS audit cycle. Planning the use of resources for a CBIS audit includes specifying the goals for the CBIS audit cycle, determining the activities that will achieve those goals, indentifying the skills needed, scheduling the activities that comprise the CBIS audit and allocating the appropriate resources in the appropriate quantities to satisfy the stated requirements.

The ability of the CBIS auditor to achieve the resource planning objectives in an appropriate manner in a particular information systems environment is related to two major factors. First, the skill of auditors, and second, the auditing tools that are available. In a traditional environment, the CBIS auditor's skill and 'tools kit' are different from those required in advanced information systems environments. In addition to the computing and manual skills and tools, associated with CBIS auditing and data processing in traditional systems environments, it is expected that the CBIS auditors require both networking skills and network auditing tools to audit advanced information systems that utilise sophisticated networking technology.

Professional skills are a composite of several factors that contribute to the overall skill levels of CBIS auditors. Three of these factors are formal training, work experience, and professional judgement. The blending of these three factors result in a particular skill level for the individual CBIS auditor. There are three categories of skills that are relevant. These three categories of skills include auditing skills, computer systems skills, and networking systems skills. The duality of CBIS auditing emphasises the need for both types of technical skills. This duality can be important during the CBIS audit resource planning echelon, as with the preceding requirements definition portion of the engagement planning process. This part of the theoretical model is illustrated in Figure 3.6.

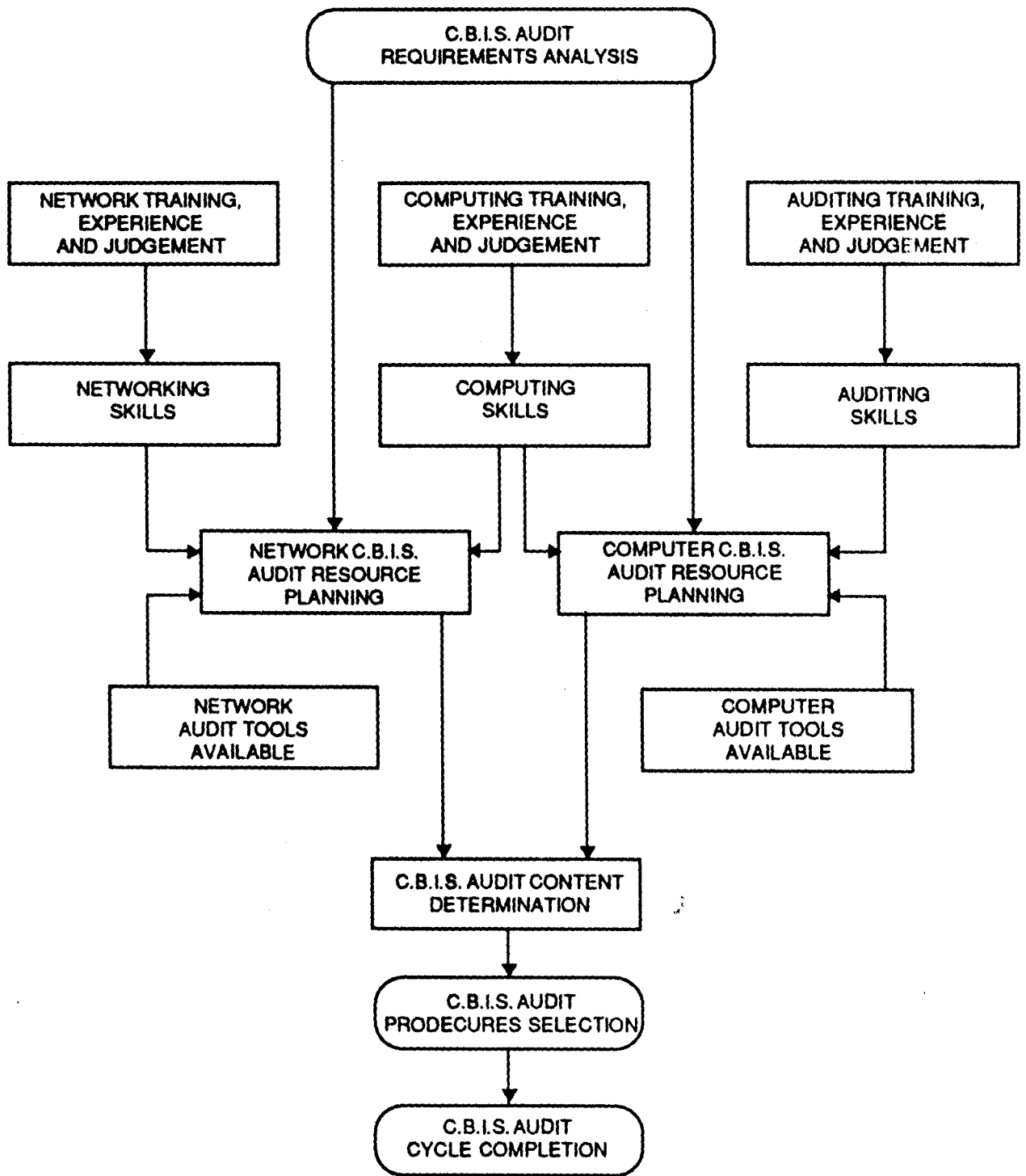
### **Part III**

#### **CBIS Audit Procedures**

The repetitive structure of the CBIS audit cycle is straight forward; and, in a stable environment, the CBIS audit cycle represents a routine, though not necessarily simple process. The critical point, particularly in dealing with longer term CBIS auditing programmes, is the selection of appropriate audit procedures for each given audit cycle.

Procedures selection includes the identification of candidate procedures that may be applicable. These candidates include standardised procedures that can be used to provide focus and direction for CBIS auditors in specific operational or technological situations, or they may include non-standard procedures that are devised by the individual CBIS auditor as applicable in a given situation.

**Figure 3.6**



**PLANNING C.B.I.S. AUDIT RESOURCE ALLOCATIONS**



Even the standard procedures are frequently adopted to each individual CBIS auditing environment. In certain situations, the appropriate set of CBIS audit activities required to perform selected audit content may not specifically relate to any generally accepted procedures. In such cases, the CBIS auditors must devise adequate new procedures to conduct the CBIS audit. As the technological complexity increases, CBIS auditors are faced with this latter situation increasingly and more frequently.

As noted in the literature review, the acceptance of new procedures depends upon a professional consensus regarding the appropriateness of each new procedure [Joyce (1976)]. Gaining acceptance tends to be a slow, conservative process. In the environment of rapidly changing technology that faces the CBIS auditor, this difference in timing means that the resource planning process, during which the audit content is specified, is increasingly critical to the overall success of a CBIS auditing engagement. In particular, the growing portion of telecommunications systems technology in information systems environment implies that developing new standardised procedures for dealing with telecommunications auditing is a CBIS auditing priority that is rising rapidly.

Computer-based information systems auditing inherently includes a significant component of administrative controls reviews. CBIS auditing is one area of auditing in which maintaining administrative and financial controls is so interdependent that reviewing key administrative controls cannot reasonably be omitted from the CBIS audit, whether internal or external. The inclusion of administrative controls both varies and widens the scope of the audit process as indicated in the previous chapter.

Once the content of a particular CBIS audit is determined, that is, after establishing what will be done during a given audit cycle, the specific CBIS audit techniques to be applied in that situation are formulated. Selecting the procedures to be used includes examining the planned content of the CBIS audit, reviewing the available techniques that can provide that content in the audit and selecting the specific CBIS auditing techniques to be applied. In general, these procedures include a mix of computing systems evaluation techniques and networking systems evaluation techniques. Achieving an appropriate balance that reasonably reflects this mix during each CBIS audit cycle is a critical objective in auditing advanced information systems environments.

The content of a given CBIS audit generally consists of one or more of the following [Davis (1974); Rittenburge & Davis (1977); Van Zutphen (1980)]:

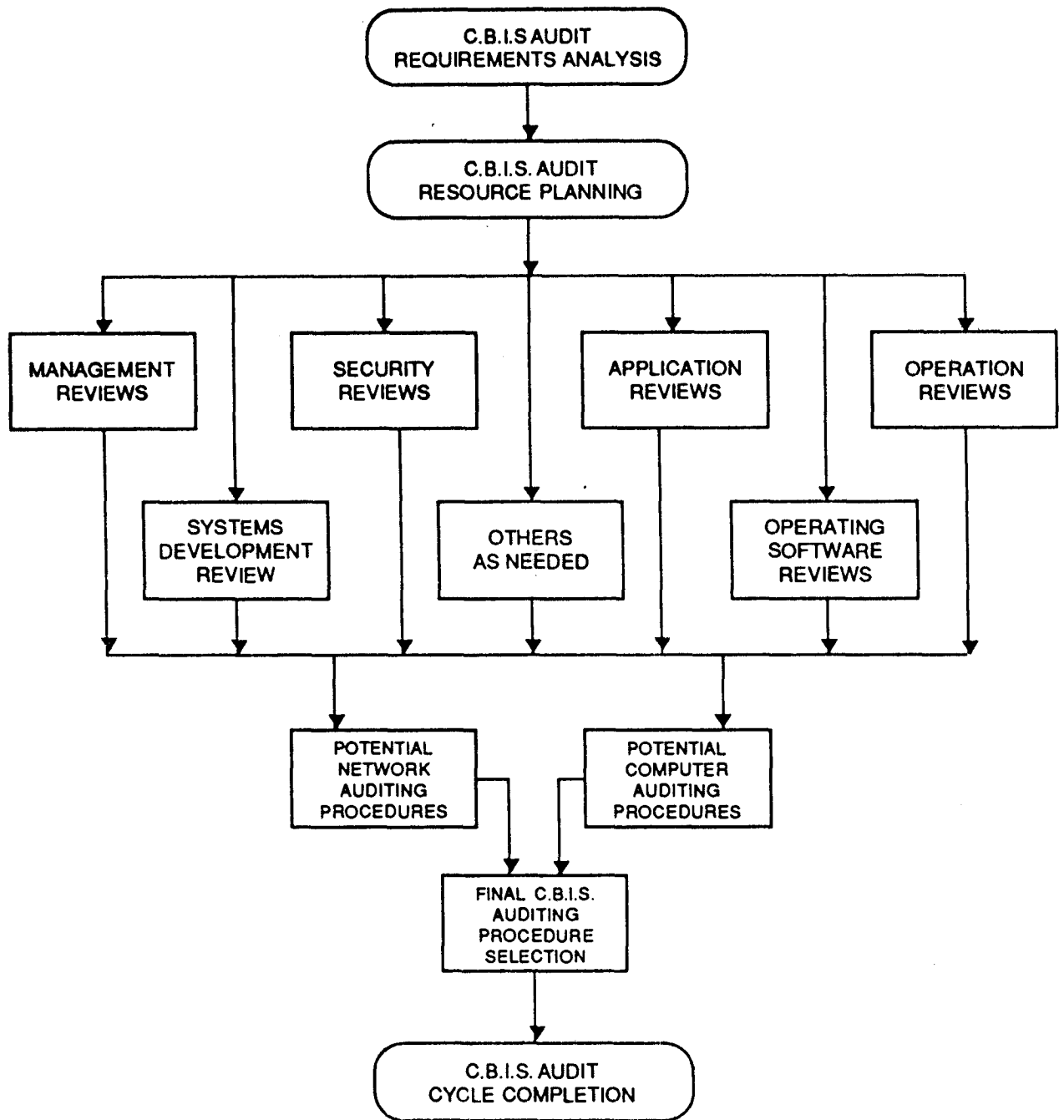
- \* Management Audit;
- \* Security Audit;
- \* Applications Development Audit;
- \* Applications Review;
- \* Operations Review;
- \* Operating Software Review.

As the subject of CBIS auditing matures, it is reasonable to expect an evolution in the content of CBIS auditing activities. This evolution will modify the categories listed above. In some cases new categories will be added. In others, the methodological content of existing categories will require significant revision.

Particularly, with regard to telecommunications network auditing, all of the categories listed above must be expanded, even if auditing a relatively simple network. Though computer and communications technologies are becoming indistinguishable electronically, much of the language and many of the concepts in telecommunications are still very different from those used in computing contexts. Thus, this expansion of CBIS audit scope will be necessary. While considering 'security audit' and 'management audit' procedures in traditional data processing vis-a-vis large-scale distributed computing network, the differences in procedures are obvious. Since, the large distributed data processing networks include several traditional data centers, numerous minicomputer installations, and various PCs as network nodes. All these require the audit procedures to be conceptually and methodologically different. In the first case, the centralisation of the data and equipment makes the control of access to the facilities and to the data itself less complex. In the second case, the geographic dispersion of access capabilities makes the CBIS auditor's analysis of controls much more difficult. Similarly, management audits conducted in these kinds of diverse situations are very different in both structural detail and content. The same is true for each audit category listed above.

Figure 3.7 shows the position of theoretical model that relates to determining which CBIS audit procedures are used in a particular audit cycle. This study is concerned with telecommunications network auditing as a growing component of the computer-based information systems audit paradigm. As with other echelons of audit engagement planning, the duality of computing and networking components in the formulation of CBIS audit techniques is a basic structural characteristic of the model.

**Figure 3.7**



**DETERMINING C.B.I.S. AUDIT PROCEDURES**

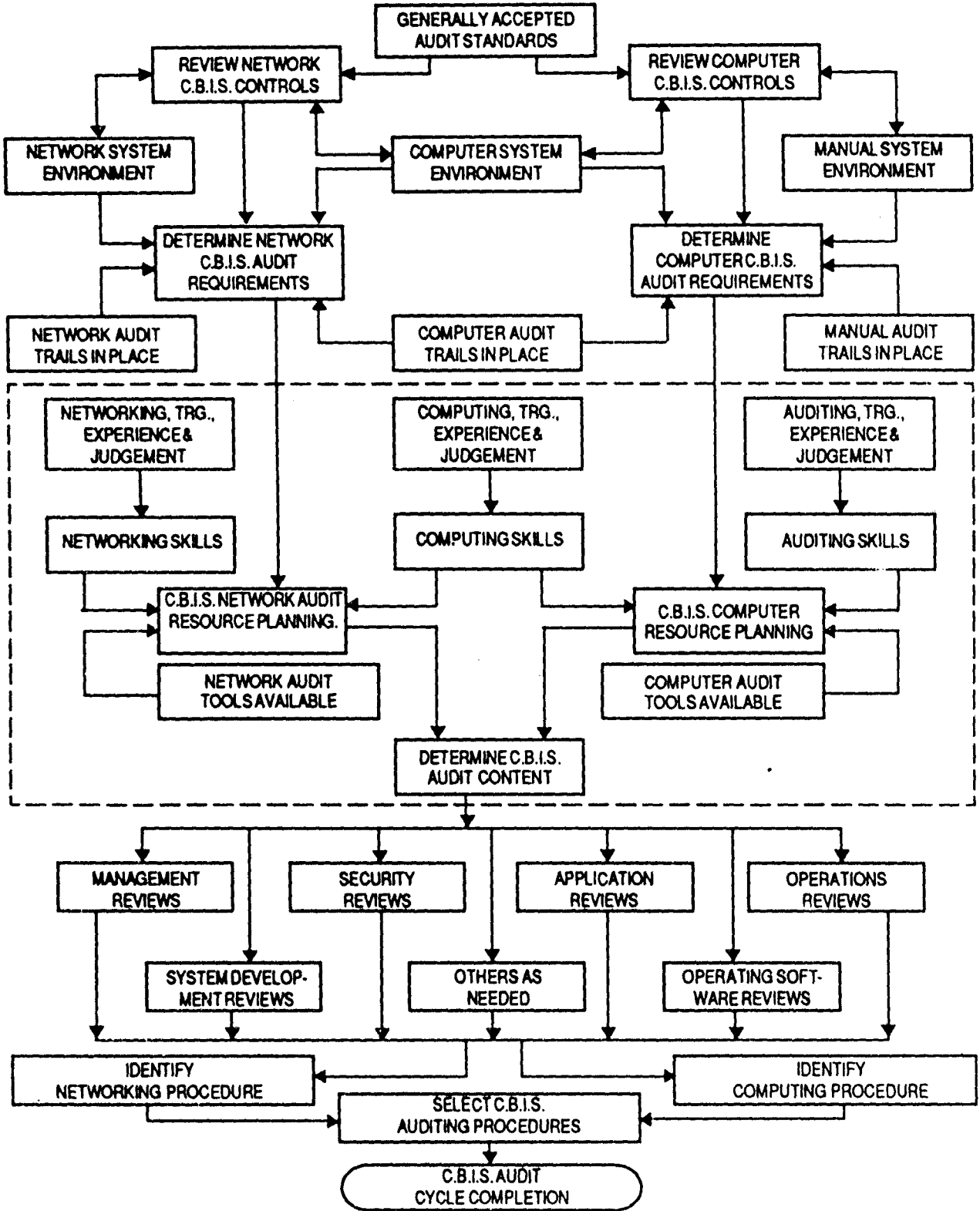
### **Theoretical Model In Brief**

The theoretical model discussed in this section has been presented as a series of related sub-models. These sub-models can be combined to arrive at one composite model that describes the overall process of CBIS audit engagement planning. By combining Figure 3.5 through Figure 3.8, the complete theoretical model can be constructed. This model features the duality of computing versus networking technology in CBIS auditing. It also exhibits the characteristic that as networking technological complexity increases in an environment, the balance between traditional computer auditing procedures and advanced network auditing procedures is represented by moving from right to left across the model in Figure 3.8.

This theoretical model represents the first three steps in a typical CBIS audit cycle as shown in Figure 3.1. It depicts conceptually how the processes of requirements analysis, resource planning, and procedures development result in the specification of activities to be done in a CBIS audit engagement. Superimposed upon this model is the capacity for various levels of iteration between the echelons, as shown in Figure 3.2.

This theoretical model provides a framework for this research in CBIS auditing. Within this research framework, the model provides the theoretical basis for a study that focuses on audit resource planning. The methodological structure of this study is described in the next chapter of this thesis.

**Figure 3.8**



**PLANNING C.B.I.S. AUDIT ENGAGEMENTS**

## **R e s e a r c h   Q u e s t i o n s**

There are three research questions proposed for examination in this research effort. They are as follows.

1. What are the critical success factors for audit planning during CBIS auditing engagements within traditional computing systems environments ?
2. What are the critical success factors for audit planning during CBIS auditing engagements within advanced computing and networking systems environments ?
3. What are the similarities and differences between the critical success factors for audit planning during CBIS auditing engagements in traditional computing systems environments versus advanced computing and networking environments?

These are important questions that deal with the very essence of CBIS auditing in an era of profound technological change. Kleinrock (1985) states that the growth of distributed systems "has attained unstoppable momentum" and that many challenging problems in distributed computing remain unsolved. How to successfully audit advanced computing and networking systems usage is one of those key problems for CBIS auditors, business managers, and executives. Answering the research questions listed above provides an initial step toward dealing with this and related problems.

By focusing on planning the allocation of resources in a CBIS audit as depicted in Figure 3.6 and similarly focusing on the critical success factors associated with computer-based information systems auditing in traditional and advanced information systems environments, a research design that provides a basis for

studying CBIS audit planning can be constructed. This design addresses the identification of those critical success factors related to audit planning for CBIS audits in advanced computing and networking environments. The design of this research is discussed in detail in the following chapter on methodology.



## **CHAPTER 4**

### **RESEARCH DESIGN AND METHODOLOGY**

A theoretical model for conducting a computer-based information systems (CBIS) audit in both the conventional computing systems environments and the complex telecommunications networking and distributed processing environments was presented in chapter 3. The duality of CBIS auditing process was emphasised within these divergent technical situations while constructing this model. This duality is basic to the research design presented below. Two analyses of critical success factors are employed into various aspects of CBIS auditing for this study.

The main theme of this research attempt is to identify and rank of the critical success factors that contribute to the effectiveness of the CBIS audit function by influencing the CBIS audit resource planning process. Within the context of this research, the terms 'effectiveness of an audit' and 'success of an audit' are considered to be synonymous. Both of these expressions reflect the degree to which the 'audit requirements' that exist during a particular audit. These expressions are addressed (and, for which objectives are achieved) by the 'audit procedures' that are actually performed during an audit cycle.

A research design and methodology for identifying and comparing factors, specifically those influencing engagement planning, that affect the level of success achieved during CBIS auditing engagements in different technological environments, is presented in this Chapter. Furthermore, the typical methodological difficulties encountered by information systems researches, as noted by

Jarvenpa et al (1985), have been considered in the design and methodology for this research. These difficulties fall into four categories : problems with research strategies, problems with research designs, problems with measurement instruments, and problems with experimental tasks. The following sections of this chapter present the strengths and weaknesses of this research effort in terms of these categories.

### **R e s e a r c h   S t r a t e g y   A n d   D e s i g n**

This research embodies an exploratory field study without experimental manipulation that investigates the relationships among individual CBIS auditor's self reported belief, perceptions, and relevant behaviours. This research includes development of an appropriate questionnaire and administration of that questionnaire to practicing external CBIS auditors and CBIS audit consultants. These 'study subjects' have good experience in this specific area in India & abroad. The data thus collected have been analysed to identify and evaluate the critical success factors for CBIS audit resource planning in traditional versus complex system environments. Critical success factors were derived by grouping component variables into statistically related categories that represented higher level constructs. These constructs were the critical success factors within the framework of this research. Finally, a comparison was made of the critical success factors for CBIS audits in the two technical environments being studied.

The series of analyses employed were accomplished using a pair of statistical techniques, first, the development of a criticality index for individual factor components (Often called 'research variables' elsewhere in this thesis) and second, the use of factor analytic techniques as listed below:

1. A criticality analysis to identify critical factor components in traditional computing environment.
2. A factors analytic examination of the factor variables in order to determine the critical success factors related to auditing traditional centralised computing systems.
3. A second criticality analysis to examine critical factor components in complex distributed data processing and networking environment.
4. A second factor analysis to determine critical success factors related to auditing of complex distributed data processing and networking situations.
5. A ranking and comparison of the critical success factors for CBIS auditing within and between each of the two technological systems environments.

Prior to describing the statistical analyses that were performed in this research, it will be helpful to present a description of the research questionnaire used to collect the data. This will provide the context within which to subsequently present the details of those analyses.

### **Data Collection Instrument**

The rationale behind the development of the instrument used in this study is explained in this section of the chapter. Firstly, the expected construct variables or categories, are defined. These categories represent the critical success factors that are focus of this research. Secondly, the individual component variables for each category are theorised. These variables provide a basis for developing the questionnaire, which is discribed in the succeeding paragraphs.

Though literature pertaining to CBIS audit provide theoretical justification, but hardly extend any empirical evidence for the proposition that certain generic factors may be contributors to the success of CBIS auditing engagements.

Unfortunately, this justification has not been well articulated in the literature, as summarised previously in this thesis. Thus, a comprehensive list of factors, that influence the success of CBIS audit engagements and that could serve as the starting point for this research, has not been previously developed. Therefore, the study of these factors required an exploratory research postures.

The literature was surveyed initially, to identify appropriate candidates for factors that appear to materially affect the success of the CBIS audit resource planning function. These candidate factors relate to the structure depicted in Figure 3.8, in that portion of CBIS audit engagement planning model which is enclosed within the dotted lines. Next, a series of discussions with a dozen of practicing external auditors and CBIS audit consultants helped to provide clarification and to finalise the candidate factors to be studied. The following seven candidate factors were thus, identified. Each has a potential of being critical or key, success factors influencing the effectiveness of CBIS audit resource planning activities :

1. Understanding of audit requirements;
2. Breadth of training;
3. Depth of training;
4. Breadth of experience;
5. Depth of experience;
6. Availability of audit tools; and
7. Quality of professional judgement.

It should be noted that though each of these items is potentially a critical success factor for CBIS auditing resource planners in the general sense, they are presented here only as a frame work within which to provide a basis for constructing the questionnaire to be used in this research. It is the objective of this doctoral dissertation effort to identify and rank, in terms of criticality, two sets of empirically-based critical success factors for CBIS auditing.

It is suggested later in this section that there are components (what might be called 'subfactors') that are related to each of these candidate critical success factors. The criticality index analysis mentioned above and described in detail below relates to determining the criticality of the individual components separately from establishing the factors that related to the components. The factor analysis, on the other hand, relates to the evaluation of components that are correlated with each other, and thus, can be interpreted as representative of higher level factors. Therefore, the criticality and factor analysis techniques together provide the methodological structure for the systematic comparison of the key factors in auditing information systems in changing technological environments characterised by increasing decentralisation.

It should be noted that other individual differences such as analytical ability, communications skills, and organisational skills are not included in this list. In order to restrict the scope of this research to the question at hand, several simplifying assumptions were needed. The assumptions here are that, as long as the auditor has an acceptable minimum level of these capabilities fluctuations in these factors should not importantly influence the success or failure of the typical CBIS audit engagement. The assumptions are based upon the preliminary infor-

mal interviews conducted by the researcher and described above. These assumptions appear to be entirely plausible.

Each item in the above list is shown in Table 4.1 along with specific references from the attached Bibliography that supporting the that items' inclusion as a candidate critical success factor in this context. Furthermore, each candidate can be decomposed into several components/subfactors that are related to the origi

### **R e s e a r c h      V a r i a b l e s**

The hypothetical relationships between components and factors shown in Table 4.2 provides the basis for the construction of the questionnaire used in this thesis. The questionnaire is the data collection instrument for this research dealing with the evaluation of critical success factors for CBIS audit engagement planners, both in traditional computing environments and complex distributed data processing environments.

Specific variable is defined in each of the component items in Table 4.2. Each variable is measured by responses of questions in questionnaire. The questions are in the form of statements about CBIS audit resource planning. The respondent is asked to indicate the extent of his agreement/disagreement with each statement as a contributor to an effective audit and the extent to which each statement describes an item that is critical to the successful execution of CBIS audit planning activities. The respondent selects one of five Likert scaled responses on each of two scales provided for each item presented and the perceived criticality of each item respectively.

**Table 4.1**  
**Candidate Factors Reference Summary**

S.N.	FACTOR	REFERENCE
1.	UNDERSTANDING OF AUDIT REQUIREMENT	ALLEN (1982) DAVIS & WETHERBE (1979) Mc FARLAN ET AL (1983) PARKER (1981) PATHAK (1988) PERRY & WARNER (1978) PORTER & PERRY (1984)
2.	BREADTH OF TRAINING	AICPA (1976) BRANSCOMB (1979) PERKINS (1983) VANECK ET AL (1983)
3.	DEPTH OF TRAINING	AICPA (1978) BRILL (1982) VAN ZUTPHEN (1980) WEBER (1980)
4.	BREADTH OF EXPERIENCE	AICPA (1976) BRANSCOMB (1979) DAVIS ET AL (1983) PERKINS (1983)
5.	DEPTH OF EXPERIENCE	AICPA (1978) DAVIS & WEBER (1903 a) PORTER & PERRY (1984)
6.	AVAILABILITY OF AUDIT TOOLS	HOLIEY & MILLER (1983) KOVACH & INSELBERG (1984) LORD (1975) PATHAK (1990) MENKUS (1985) WASSERMAN (1969)
7	QUALITY OF PROFESSIONAL JUDGEMENT	ACKOFF (1970) JOYCE (1976) JOYCE & LIBBEY (1982) NOLAN (1982) NORRIS (1983) PERRY (1985) TROTMAN YETTON (1985) PATHAK (1991)

**Table 4.2**

**COMPOSITION OF CBIS AUDIT RESOURCE PLANNING FACTORS**

**FACTOR 1 UNDERSTANDING OF CBIS AUDIT REQUIREMENTS**

1. Define Objectives For Each Situation.
2. Evaluate The Relevance And Materiality of Each Planned CBIS Audit Activity.
3. Review Completeness of Each CBIS Audit Plan Based Upon Individual Situation.
4. Document The Plan For Each CBIS Audit Prior To Beginning The CBIS Audit.

**FACTOR 2 BREADTH OF TRAINING**

1. Train CBIS Auditors In General Auditing Concepts And Analytical Techniques.
2. Train CBIS Auditors In Applications System Concepts And Programming Techniques.
3. Train CBIS Auditors In Operating Systems Concepts And Programming Techniques.
4. Train CBIS Auditors In Computer Operations Concepts And Supervisory Techniques.
5. Train CBIS Auditors In Data Base Systems Concept And Data Management Techniques.
6. Train CBIS Auditors In Time-sharing Concepts And Applications Techniques.



**7. Train CBIS Auditors In Computer Network Concept And Telecommunication Systems Technology.**

**8. Train CBIS Auditors In Distributed Processing Concepts And System Technology.**

**9. Train CBIS Auditors In Information Systems Management Concepts And Methodologies.**

### **FACTOR 3 DEPTH OF TRAINING**

**1. Provide Advanced Training for CBIS Auditor. In General Auditing Techniques.**

**2. Provide CBIS Auditors with Advanced Systems Training In Computer Operation, Application System, And Management.**

**3. Provide Advanced Training for CBIS Auditors In Telecommunication Network Technologies.**

### **FACTOR 4 BREADTH OF EXPERIENCE**

**1. Expose CBIS Auditors to Projects Involving General Auditing Assignments.**

**2. Expose CBIS Auditors To Projects Doing Application System Development work.**

**3. Expose CBIS Auditors To Projects Involving Operating system Programming Tasks.**

**4. Expose CBIS Auditors To Projects In Computer Operations.**

**5. Expose CBIS Auditors To Projects of Data Base Systems Development Work.**

6. Expose CBIS Auditors To Networking Using Telecommunication Technologies.
7. Expose CBIS Auditors To Time-sharing & On-line Projects.
8. Expose CBIS Auditors To Distributed Processing Systems Project work.
9. Expose CBIS Auditor To Projects Involving Information Systems Managements Tasks.

#### **FACTOR 5 DEPTH OF EXPERIENCE**

1. Utilise Technical Specialists In Information Systems Auditing.
2. Utilise Technical Specialists In Computing System Technology.
3. Utilise Technical Specialists In Telecommunication Net-working Technology.

#### **FACTOR 6 AVAILABILITY OF AUDIT TOOLS**

1. Provide Standardised CBIS Audit Methodologies, Procedures And Techniques.
2. Provide Access to A Wide Range of Technical Library Reference Material.
3. Provide Software For Usage Reporting.
4. Provide Software/Hardware Monitors.
5. Provide Models For Data Reduction, Forecasting, And/or Systems Simulation.

## **FACTOR 7 QUALITY OF PROFESSIONAL JUDGEMENT**

- 1. Review Decisions Regarding CBIS Audit Engagement with Non-CBIS Audit Personnel.**
- 2. Establish Proper Mix of Personnel And Skills To Cover All Categories of Necessary Expertise For Each CBIS Audit.**
- 3. Utilise Participative Management Approach In Supervising And Directing The Activities of The CBIS Audit Team.**
- 4. Assure That Long Term Audit Perspective Is Actively Considered In The Short Term Planning of Each CBIS Audit.**

Each variable, as represented by a statement on the questionnaire, also appears identically in each of the two sets of questions, one assuming traditional computing systems environment (called scenario A) and one assuming complex distributed data processing and networking environment (called scenario B). A copy of the questionnaire developed for use in this research is shown as the attached appendix. Further descriptions and examples of the constructs outlined in Table 4.2 above and the associated research questionnaire items are presented in the following pages.

### **Understanding of Audit Requirements**

The definition of audit requirements in a CBIS audit engagement is analogous to the definition of programming requirements during the systems development life cycle (SDLC) for a typical application software project. If the requirements definition is poorly done, then the functional content of the resulting software is unlikely to produce satisfactory operating results and unlikely to be perceived

as a success by management [Helms (1983)]. Similarly, lack of attention to technical audit requirements during CBIS audit resource planning poses problems for the successful completion of an audit. Each technical environment for information systems processing, whether or not it includes complex networking components, inherently exhibits its own, perhaps even unique, audit requirements. It is the responsibility of each audit resource planner to recognise the salient characteristics of each CBIS audit situation and to devise an appropriate functional content for the audit that has a high likelihood of successful completion by the available audit staff.

It is expected that this construct includes four components (or variables). The first is the importance of establishing objectives for each CBIS auditing situations. Research findings should indicate whether the CBIS auditor should establish objectives in advance for each audit situation or should attempt to discover the appropriate set of objectives as the audit engagement unfolds.

The second component deals with the importance of evaluating the relevance and materiality of planned audit activities. In other words, should CBIS audits be customised to the situation or follow mostly standardised procedures in evaluating the use of information technologies in specific situations?

The third component considers the importance of completeness of the planned CBIS audit for a specific technical environment. Should CBIS auditors determine whether a technical audit programme is appropriately thorough during a particular audit cycle or should they only follow standard technical procedures without concern for questions of completeness that are contingent upon the particular situation?

The fourth component relates to the importance of documenting the CBIS audit plan in enough detail to serve as a control document for the management of the audit cycle. Should a formal audit plan be established prior to the beginning of the audit or should less formal, more unstructured approaches be employed to facilitate flexibility and adaptability during the audit process?

### **B r e a d t h   o f   T r a i n i n g**

Training in this context deals with the technical training in computing, networking, and auditing, to the extent that an individual's formal education contributes to his technical training. Education related to each of these areas is considered to be a form of training and is included in this category. It is reasonable to expect that the breadth of the CBIS audit resource planner's training in computing, networking, and auditing has a material influence upon the eventual content of the audit, and thus, upon the ultimate success of the audit engagement. It is also reasonable to expect the training needed for planning audits in more complex computing and networking situations.

Hence, the breadth of training construct consists of nine parts, each of which deals with a specific area of technology that often arises in the context of an audit. How important is training in each area for the CBIS auditing professional? These components deal with technical training related to general auditing, applications systems and programming, operating systems concepts, computer operations issues, data-base and data management techniques, time-sharing applications, computer networking and telecommunications, distributed processing, and issues pertaining to the management of information systems technology.

## **D e p t h o f T r a i n i n g**

It is plausible that the technical depth of the training should be appropriate to the situation. In order to achieve effective audit resource planning, the planner needs exposure to the technical details regarding the computers, networks, and auditing itself, as three-some-what distinct and separate technologies. In the absence of these technical bodies of knowledge, the scope of the audit is subject to being artificially limited, resulting in the arbitrary omission of potentially key areas of functional content for a given audit. Such omissions seriously limit the potential for success of the CBIS audit engagement.

It is expected that this construct includes three components. The first deals with the importance of advanced in-depth training for computer-based information systems auditors in financial auditing techniques. Research findings may indicate whether CBIS auditors should be trained as audit professionals or be systems professionals with a limited knowledge of auditing.

The second component focuses upon the importance of advanced computer systems training in CBIS auditing situations. Should the CBIS auditor be a bona-fide computer systems expert or should the CBIS auditor be computer literate but not necessarily expert in the technology?

The third component relates to the importance of providing advanced training to CBIS auditors in computer networking and telecommunications systems technology. Should the CBIS auditor be concerned with networks or is the conventional approach concentrating primarily upon computing systems technology sufficient for computer-based information systems auditing?

## **B r e a d t h   o f   E x p e r i e n c e**

Experience in this context refers to experience of working with the various aspects of computer systems, network systems and technical auditing activities. It is reasonable to expect that a wide range of experience in these technologies has a positive influence on the CBIS audit resource planning function. Familiarity with the practices followed in differing information systems environment, regarding computing, networking, and auditing helps the audit planners to evaluate the resources needed to conduct a successful auditing engagement.

It is anticipated that the breadth-of-experience construct includes the same nine components as the breadth of training construct, except that the issue here is to evaluate the importance of project experience in each of the technical areas cited above in CBIS auditing. Should a CBIS auditor have a wide range of technical experience to draw upon during an audit or is it sufficient for the auditor to generalise based upon limited experience?

## **D e p t h   o f   E x p e r i e n c e**

It is also reasonable to expect that the technical depth of the CBIS auditor's exposure to the technologies of computing, networking, and auditing influences his capability to successfully plan the content of a CBIS audit. Depth of experience, as with depth of training, contributes to the audit resource planner's ability to achieve an appropriate scope for the audit by avoiding inappropriate restrictions on audit content due to gaps in relevant areas of technical knowledge. Depth of experience should help the planner to achieve the appropriate content in the audit resource allocation planning process.

It is expected that this construct is composed of three component parts, each of which relates to the importance of technical specialisation in CBIS auditing. In-depth technical experience relates to the development of technical specialists among CBIS auditors. The three technical specialities noted are auditing technology, computing systems technology, and telecommunications networking technology. Should computer-based information systems auditors develop technical specialities in these areas or should they be generalists with minimal

### **A v a i l a b i l i t y   o f   A u d i t   T o o l s**

Audit tools include many resources that are utilised by the CBIS auditor to perform specific tasks. These include computer-based tools such as hardware and/or software monitors or utilisation reporting programme and other tools such as technical reference materials or standard methodologies for conducting CBIS audits in various situations. The applicability of specific tools in specific situations tends to depend upon each situation; and it is reasonable to expect that the availability of audit tools in a given environment is an important contributor to the success of a CBIS auditing effort, particularly in more advanced computing and/or networking environments.

The 'availability-of-audit-tools' construct decomposes into five components. The first deals with the importance of providing CBIS auditors with standardised auditing procedures, techniques, and methodologies. Research findings should indicate whether computer-based information systems auditors should base audits upon standardised audit approaches or customise various approaches depending upon the situation in each individual audit.



The second component relates to the importance of providing the CBIS auditor with access to a library of technical reference materials. Should the auditor rely upon standard procedures, education and experience, and client information sources only or should the CBIS auditor utilise a technical reference library to supplement other technical information sources?

The third component involves the importance of having access to appropriate report software for use in conducting a CBIS audit. Should the CBIS auditor be able to extract audit reports from the systems being audited or should the auditor rely upon client reports and personnel to provide the needed reports?

The fourth component regards the importance of having access to hardware and/or software monitors as tools for use during a CBIS audit. Should the auditors have access to system monitors or should they rely upon the client personnel for system information both current and historical?

The fifth component deals with the importance of using models to facilitate the audit process by summarising the volumes of data needed, forecasting significant trends, and simulating systems operations. Should the CBIS auditor utilise such modeling tools, or should the information needed be extrapolated using less sophisticated methods?

### **Quality of Professional Judgement**

The professional judgement of auditors is an important dimension of any auditing situation. In CBIS auditing, there are three technical areas within which professional judgement is exercised; these are computing, networking, and audit-

ing. Judgements formulated in these three areas tend to be independent because they each rely upon different knowledge bases. However, these kinds of judgements are all interrelated within the context of the individual audit engagement. It is, therefore, reasonable to expect that the technical judgements made by the CBIS audit staff generally affect the potential for success of the audit. It is also plausible that poor judgements by audit engagement planners decreases the likelihood of a successful CBIS audit.

It is expected that this construct includes four components. The first deals with the importance of coordinating the CBIS portion of an audit with other parts of the audit process. Internal or external, financial or operations auditing activities are frequently related to CBIS auditing activities. Should CBIS auditors make decisions in an isolated, closed manner or should the CBIS auditors actively solicit information and opinions of non-CBIS personnel engaged in other aspects of an audit?

The second component relates to the importance of establishing the proper skill mix to assure that the expertise needed to conduct an audit in a specific situation is included among audit team members. Should the CBIS auditors concentrate the technical audit decision-making only on areas in which the audit team has established expertise or should the auditor supplement the audit team with technical specialists who can provide additional understanding as needed?

The third component involves the use of participative management to derive leverage from the technical judgement capability of the audit team as a whole. Should the lead auditor make the technical decisions related to the audit or

should the audit team utilise consensus seeking techniques to arrive at technical decisions affecting the audit?

The fourth component of this factor deals with the importance of the temporal context of technical decision-making. Should technical judgements made during a CBIS audit include consideration of longer-term audit planning or should they focus only on the short-term planning conducted within each audit cycle?

On the basis of the initial candidate factors described above and that were drawn from the literature review and theoretical issues presented previously in this thesis, a questionnaire was constructed and used to collect the data that provided the basis of this research. That data was analysed and the results included an empirically based identification of actual critical success factors attributable to planning of CBIS audits in both traditional centralised computing systems environments and complex networking and distributed computing environments. The processes of data collection and data analysis that were utilised in this research are summarised in the next section of this thesis.

### **Data Collection And Analysis**

The questionnaire instrument as shown in the appendix to this thesis administered as a pretest to CBIS auditors located in NEW DELHI Metropolitan area. Subsequent to the pretest and after completion of modification to the questionnaire it was administered to the practicing CBIS auditors and consultants in CBIS area in the metropolitan cities of Delhi (including New Delhi), Calcutta, Bombay & Madras. All subjects for this study were professional external auditors & consultants employed by the international/national level chartered account-

ants' firms/franchise in India. The questionnaire was administered to external auditing personnel only. The questionnaire survey instrument was administered once only to the target population of subjects to collect the data for this research.

This research includes two essentially distinct groups of data, one for identifying and ranking factors in traditional computing environments (Scenario A) and one for identifying and classifying factors in complex networking distributed data processing environments (Scenario B). Furthermore, there are two Likert scales for each questionnaire item the agree/disagree and the critical/non-critical scales. All analyses described in this section utilised the data associated with the agree/disagree scale, with the exception of the criticality index computation described below.

These groups of data were analysed using the Statistical Package for Social Sciences (SPSS). Pair-wise tests were run to test statistically each variable for the differences between data collected assuming Scenario A versus that collected assuming Scenario B. Different procedures were utilised to develop appropriate descriptive statistics for the variables under investigation particularly for use in the development of the criticality indices and for the demographic data summary statistics.

In this thesis, the construct variables are the critical success factors for CBIS auditing. As noted by Kerlinger (1973), factor analysis can be regarded as a methodological link between measurement theory and factor theory, as a tool for assessing construct validity. Also, Mitchell (1985) suggests that construct validity is a broad concept embracing dimensions of both predictive validity and concur-

rent validity. Thus, within the design of this research, factor analysis provides the methodological frame work for transforming a collection of measurements into valid factor constructs and for both validly assessing concurrent critical success factors that affect planning for CBIS auditing engagements.

Several factor analytic procedures employing the principal components method with orthogonal rotation (using the varimax criterion) provided the basis for extracting the critical success factors from the data. This method of analysis is often used in this type of study as exemplified by [Ginzberg (1981), Morrison (1983), and Rushinek & Rushinek (1984)].

Factor analysis is a method for determining the number and nature of underlying variables among a larger collection of measures [Kerlinger (1973); Kim & Muller (1978 a & 1978 b)]. It is a method for extracting common factor variance from among the sets of associated measures. Factor analysis results in a factor matrix containing coefficients that, like correlation coefficients range between -1 & +1.

These coefficients can be interpreted as correlations between the measurement variables and the underlying factors. It is said that individual variables "load" onto certain factors depending upon the magnitude of these coefficients (also called "factor loadings"). They express the relationships between individual component measures, in this case responses to the questionnaire items, and hypothetical construct variables that represent the higher order factors.

## **Assessing Component Differences**

Each of the thirty-seven variables under study in this research appeared in the questionnaire instrument once under Scenario A and once under Scenario B. Every variable was associated with an identical statement for each scenario, though the order of the statements within the scenarios was fully randomized. Pair-wise t-tests were used to systematically compare the mean responses (on the agree/disagree) data for each variable in the set of matched questionnaire items. Those means that were statistically significantly different (at the .05 level) were identified. The results of this analysis are presented in the next chapter of this thesis.

Each of the data analysis techniques summarised briefly above is described in further detail in the following sections.

### **Determining Component Criticality**

The questionnaire instrument employed for data collection during this research included two five (5) point Likert scales per questionnaire item. On the second scale, the respondent was asked to indicate the level of criticality for successful CBIS auditing for each questionnaire item. The scale ranged from "Non-Critical For Success" (1) to "Critical For Success (5).

The set of data collected from this "Criticality assessment scale" provided the basis for developing an index that could be used to judge the relative importance of various questionnaire items (and the related factor components, or variables, in this research). To develop such a scale, the data was transformed

from the Likert scale to a binary format consisting only of "non-critical" or "critical" designations.

Responses of one, two, or three on the five point scale were transformed to zero (representing responses of "non-critical" or "neutral"); responses of four or five were transformed to one (representing responses of "critical"). The mean responses for each variable using the transformed data gave a relative criticality index (ranging between zero and one). This index reflects the collective judgement of the research subjects regarding the overall criticality of components associated with the questionnaire item in the two CBIS auditing situations under investigation as outlined previously.

The criticality index was utilised in this research to assess the relative criticality of individual factor components. Clearly, the index is an overall approximation based upon the set of responses collected during this research effort. The level of criticality for a specific component will vary depending upon the particular CBIS auditing situation encountered. Still, assuming that the data collected was representative of questionnaire items, several generalisations were plausible.

For example, an index of 0.50 or greater meant that at least 50 percent of the respondents indicated that the related component was critical to the successful planning of CBIS audit engagements. Therefore, for each factor component in the subsequent analysis, an index of 0.50 or higher was critical. An index that was less than 0.50 was likewise non-critical. Also, the higher the value of the index for a given factor component, the higher the overall criticality associated with that component.

## **Extracting Critical Success Factors**

In conjunction with the pairwise t-test analysis and the criticality index analysis, a factor analysis of the agree/disagree data was utilised to structure each group of factor components into a logical hierarchy. By grouping the factor components together statistically, it is possible to construct higher level variable. Within the context of this research, each higher level variable is defined to be a critical success factor construct. This is a natural consequence of the structure of the questionnaire and the factor analytic process.

The results of the factor analysis will allow the audit planner to focus on a parsimonious set of topics, to direct planning activities toward a minimal number of major issues rather than a large number of seemingly unrelated component issues. Arriving at both the appropriate constructs and the appropriate component variables for each construct in this manner gives the audit planner important new capabilities in structuring audit activities. These constructs potentially provide the framework for systematically organising, planning, and controlling CBIS audits.

Understanding the critical success factors that relate to resource planning for CBIS audits provides the audit planner with the insight necessary to achieve increased audit effectiveness. Allocation of the appropriate resource for a given audit situation, adequate technical training for the audit staff in the techniques of computing, networking, and auditing, focusing of audit activities on the appropriate topics for an effective audit in a given technical environment and improved management control of the audit situation are potential benefits of this understanding.



## **Comparing Technical Environments**

Four types of data analysis techniques were utilised during this research effort. First, a series of paired t-tests determined the variables for which data collected under scenario A were statistically significantly different (at the 0.05 level) from data collected under scenario B. Then, the criticality index analysis was used to establish the relative criticality among the component variables within each processing environment. Next, the factor analysis provided the grouping of the related components into appropriate categories that result in the critical success factor constructs. Finally, the composite criticality indices were constructed for the factors providing an empirically derived estimate of their relative criticality. Each of these analysis established a basis for the comparison of critical success factors under differing technological assumptions.

- By constructing one set of these factors for CBIS audit engagement planning in traditional computing environments and one for complex distributed data processing and networking environments, it became possible to perform a systematic comparison of the resulting two sets of factors. This analysis involved comparisons of what components were included in which factors both within and
- between processing environments what components were perceived as critical by CBIS auditors in which situations, the level of criticality of individual components and the relative importance of the critical success factors in the two different environments being studied in this research. The complete results of the analyses described in the preceding paragraphs are presented in the next chapter of this thesis.

## **SUMMARY**

**This thesis includes three different, but related, analyses of data collected in essentially two parallel field study research efforts. The first analysis involves determining the critical success factors that are associated with CBIS audit planning in traditional information systems environments from the perspective of the professional CBIS auditor. The second analysis involves determining similar factors for advanced information systems environments with complex distributed data processing networking facilities. The third analysis includes the systematic comparison of the findings of the first two analyses in order to identify similarities and differences between factors that apply in each CBIS auditing situation. This comparison will provide a basis for assessing the extent to which the two kinds of information systems environment may require different approaches to CBIS auditing. Because of the limited basis of empirical research in the computer based information systems auditing field, the first two analysis are necessary to provide a basis for addressing the third analysis, which is the primary emphasis of this doctoral thesis.**

## **CHAPTER 5**

### **ANALYSES AND INTERPRETATIONS**

This chapter presents results of analysis that were performed using data collected by administering the questionnaire included in the appendix of this thesis. That instrument solicited opinion relating to the thirty seven (37) research variables discussed in the preceding chapters. The data was collected from the subjects as described in the last chapter. The rest of this chapter is divided into nine (9) major sections. The first section describes the aggregate demographic characteristics of the respondents. The second section presents the results of the tests performed on matched pairs of questionnaire responses. Responses to questions dealing with conventional centralised processing environments (Scenario A) are compared with the corresponding questions dealing with complex computing and networking environments (Scenario B). Significant differences are reported and discussed.

The next major section of this chapter describes the results derived from the use of the questionnaire's criticality Likert scale as a basis for the assessment of the criticality of each variable in the Scenario A and Scenario B environments. The relative criticality index, of each variable in the two environments is subsequently presented.

The remaining sections deal with the results of the factor analysis of the data collected. First, the various statistics that test the appropriateness of factor analysis are discussed. Next, the Scenario A critical success factors which are the results of the factor analysis on the Scenario A data are presented, followed by a results of the two factor analysis are then compared, contrasted, and evaluated

in terms of the overall criticality of each factor with each scenario. Finally, the critical success factors derived for each scenario are ranked in descending order of criticality relative to one another.

### **R e s e a r c h S u b j e c t s**

Questionnaires were mailed to 324 auditors & audit consultants who were employed by 10 large size firms of auditors. Of these, 44 questionnaires could not be delivered for various reasons. Among the remaining questionnaires, 109 usable responses were received, for a 39 percent response rate.

Respondents aged on average 34.7 years, were 24.1 percent female and 75.9 percent male; had been in employment for 5.0 years on average; had been in their current positions for an average of 2.4 years; and were approximately and evenly divided among managerial (Partners/Managers) and technical analyst position levels within the firm.

Furthermore, all respondents had completed a college Degree education, with 50 percent having received advanced degrees like M.Com/LL.B/Ph. D., etc. Predominantly respondents were Commerce graduates or post-graduates in Management studies.

But, 25 percent had the technical/scientific education at college level. Certification attained by all of them fell into two categories; first 30 percent had completed C.A. (Inter) examination of Institute of Chartered Accountants of India only, rest 70 percent had successfully finished Inter and Final examination of the same institute. But, of the total respondents, some 40 percent had done graduate level

examination of ICWAI (Institute of cost & Works Accountants of India) or ICMA (Institute of Cost & Management Accountants - U.K.) and 30 percent had acquired a graduate level qualification of the Institute of Company Secretaries of India (ICSI). Almost, everybody had undergone a course or two conducted by the computer Society of India (CSI) or other similar body or Computer education agency.

Table 5.1 summarises the demographic data that is explained above. In addition to table 5.1, table 5.2 and 5.3 provide summaries of respondent work experience and level of technical expertise. Collectively, table 5.1 through 5.3 present summaries of all demographic data that was collected as a part of this research effort.

Respondents were all engaged in CBIS auditing as a profession and were regionally and widely dispersed, providing a cross-section of responses from virtually all the major economic/commercial centers of India. As a group the respondents reported having participated in 3119 computers-based information system audit engagements since 1985, with an average level of experience per respondent of 29.4 engagements.

With regard to the respondents work experience, it is clear that the group of respondents collectively constitutes a highly experienced work force. More than 1/4th of the respondents indicated having in excess of 15 years of professional experience (including the articleship experience). Only about 20 percent indicated less than 5 years experience. Furthermore, half of the respondents reported that their professional experience focussed mostly upon computer-related work

**Table 5.1**  
**SUMMARY OF RESPONDENTS' DEMOGRAPHIC DATA**

S.N.	Description etc.	Statistics
1.	Mean Tenure With Firm	5.02 years
2.	Mean Position Tenure	2.37 years
3.	Mean Age	34.67 year
4.	Job-level :- (A) Managerial (B) Technical Audit	45.9 percent 54.1 percent
5.	Gender: (A) Male (B) Female	75.9 percent 24.1 percent
6.	Educational Attainments: (A) Under Graduates (B) Graduates/Post Graduates Law Graduate (C) Doctoral Degree	50.0 percent 45.4 percent 4.6 percent
7.	Relevant Educational Attainments: (A) Associate/Fellow of ICAI (B) Chartered Accountants Exam (Inter) passed (C) Certified Financial Analysts (India) (D) Associate/Fellow of ICWAI/ICMA (E) Associate/Fellow of ICSI	69.0 percent 24.0 percent 16.0 percent 32.0 percent 53.0 percent

**Table 5.2**  
**SUMMARY OF RESPONDENTS' WORK HISTORY**

S.No	Description etc.	Data in percentage
1.	<b>Work Experience:</b> (A) Less than 2 years (B) 2 to 5 years (C) 5 to 10 years (D) 10 to 15 years (E) Above 15 years.	11.0 19.3 26.6 17.4 25.7
2.	<b>Focus of Work:</b> (A) Mostly Acctty. & Commerce Background (B) Mostly Acctty. & Mathematics Computing Background (C) Mostly Scientific/Technical Background	21.3 29.1 49.6
3.	<b>Respondents' Roles:</b> (A) Manager/Controller etc. (B) Audit Project Leaders (C) Technical Analyst (D) EDP Acctty. Controls Splst. (E) EDP General Controls Splst. (F) EDP Applications Controls Specialist (G) EDP Administrative Controls Specialist (H) Computing Technical Expert (I) Networking Technical Expert	47.7 42.2 36.7 53.2 67.0 63.3 50.5 28.4 13.8
4.	<b>CBIS Audits Done Since 1985</b> (A) Average Audits/Respondent (B) Total Audits done by all	29.4 3119.0

**Table 5.3**  
**RESPONDENTS SELF-REPORTED LEVELS OF EXPERTISE**

S.No	Description etc.	Level in percentage		
		Low	Medium	High
1.	Application Programming	15.6	30.3	54.1
2.	Computer Operations	15.9	43.0	41.1
3.	Computer Resource Mgmt.	36.7	41.3	22.0
4.	Data Base Administration	31.2	58.7	10.1
5.	Data Network Mgmt.	49.5	40.4	10.1
6.	Data Network Operations	48.6	41.3	10.1
7.	Info. Systems Planning	18.3	32.1	49.6
8.	Procedures Analysis	19.3	34.9	45.8
9.	Op. Systems Programming	57.8	31.2	11.0
10.	Systems Analysis	14.7	33.0	52.3
11.	Systems Documentation	11.0	33.0	56.0
12.	Financial Auditing	28.4	27.5	44.1
13.	CBIS/EDP Auditing	9.2	33.0	57.8
14.	Financial Accty.	17.4	40.4	42.2
15.	Managerial Accty.	16.5	40.4	43.1
16.	Data Processing Security	13.0	33.3	53.7



while 29 percent indicated that their work experience consisted of an approximately even mixture of computing and manual accounting assignments. Only about 21 percent of the respondents indicated that their experience basis was primarily manual accounting-related. Respondents were also asked to indicate the roles that they had filled on CBIS auditing engagements. Because of the large proportion of managerial respondents noted above, it is not surprising that 42 percent and 48 percent of the respondents indicated that they had served as project leaders/managers of CBIS auditing engagements. The roles related to the various categories of EDP (or CBIS) audit controls specialists had each been filled by over 50 percent of the respondents. Of these, the EDP general controls specialists category was ranked highest with 67 percent of respondents. Only 37 percent of respondents had filled the role of technical analyst; 28 percent, the role of computing technology specialist and 14 percent, that of networking technology specialist. These statistics are summarised in Table 5.2.

Respondents were also asked to indicate their own level of expertise in 16 technical areas that relate either directly or indirectly to the ability to conduct CBIS audit engagements. A summary of these self reported estimates of levels of expertise are shown in Table 5.3. For six of the categories, more than 48 percent of the respondents rated their own expertise as "high". These were CBIS Auditing systems Documentation, Applications Programming, Data Processing Security, Systems Analysis, and Information Systems Planning. For three of the categories, more than 48 percent of the respondents rated their own expertise as "Low". Those were Operating System Programming, Data Communications Network Management, and Data Communications Network Operations. The full spectrum of responses is presented in Table 5.3.

## **Paired Responses Between Scenarios**

It was found that 21 of the 37 component variables under consideration in this study exhibited statistically significant differences (using pairwise t-tests at .05 level of significance) between means for data collected assuming Scenario A versus means for data collected assuming Scenario B. Of these, 19 variables had higher responses (a higher level of agreement indicated with the corresponding questionnaire items) for Scenario B data. Only two were higher for Scenario A data. Sixteen (16) variables did not reflect any significant differences between Scenarios A and B. Table 5.4 shows the detailed results of this analysis.

Eight (8) variables for which Scenario B responses were significantly higher dealt with experience/training related to Communications, on-line systems, or distributed processing (these included the components 1,3,13,19,20,24,25, and 33 in Table 5.4). Given the nature of Scenario B these significant differences with Scenario A responses are to be expected. Likewise, those variables that dealt with more advanced levels of technical computing expertise were expected to follow the same pattern for the same reason; six (6) variables were of this type (Components 5,15,16,21,34, and 35 in Table 5.4). Three of the remaining five (5) variables in this group dealt with resource availability in a CBIS audit engagement (Components 12,28, and 32 in Table 5.4). It is clear that additional resources are needed in a more technically complex processing environment.

Component 6 (Six) of Table 5.4 is "Review Audit Plan Completeness". Statistical significance with higher Scenario B responses indicates that reviewing completeness in a complex networking and distributed computing environment is more necessary than in the traditional Centralised computing environment of Scenario

A. Finally, component 14 (Fourteen) in Table 5.4 is "Have Non-CBIS Audit Experience". A statistically significant higher mean score under Scenario B is likely to be related to the perception that persons with strong computing and/or technological backgrounds tend to be less well versed in the techniques of auditing as explained in Chapter 3 of this thesis.

As noted, only two of the thirty-seven variables resulted in statistically significant higher values for Scenario A data than for Scenario B. These were "Review Audit-Plan Relevance" and "Have Standard Audit Methods" (Components 8 and 36, respectively in Table 5.4). These responses are apparently related to the higher availability of such methods for the traditional centralised computing (Scenario A) environments as compared to the generally more complex Scenario B environments, and to the perceived need to verify that the methods selected for a given CBIS audit are indeed relevant for that audit.

Perhaps the most interesting result of this particular analysis is the act of variables that were not statistically significantly different from Scenarios A and B (Components 2,4,7,9,10,11,17,18,22,23,26,27,29,30,31 and 37 in Table 5.4). Because of the high number of respondents (N = 109), this set of variables constitutes a consensus among respondents regarding the minimum set of component variables that is needed to conduct CBIS audits across a wide spectrum of processing environments. It is interesting to note that only one of these deals with the specific requirements of technical staff experience, that being "Have Applications Development Experience". The rest deal extensively with training and various aspects of the management of CBIS audit engagements.

**Table 5.4**  
**PAIR-WISE T-Tests BETWEEN SCENARIOS A AND B**

Note :- N=109; "\*" indicates significant difference at .05 level.

S.No.	MEAN COMPONENT	MEAN RESPONSE		T-Value
		(Scenario A)	(Scenario B)	
1.	Having Advanced Communications Training	3.0459	3.8991	- 6.72*
2.	Use Participative Mgmt.	4.0642	4.1284	- 0.79
3.	Use Comm. Tech. Specialists	3.7339	4.4037	- 5.93*
4.	Have Advanced Non-CBIS Trg.	3.2936	3.2018	+ 0.88
5.	Have Comp. Operators Expce.	1.7982	2.0183	- 2.33*
6.	Review Audit Plan Completeness	4.2018	4.5963	- 4.85*
7.	Have Adv. Comp. Training	3.8349	3.9541	- 1.27
8.	Review Audit Plan Completeness	4.5138	4.3119	+ 3.32*
9.	Have DB Mgmt. Training	3.2202	3.4128	- 1.84
10.	Have Applications Devp. Experience	3.0642	3.1927	- 1.23
11.	Assure proper Mix of staff skills	4.4037	4.4862	- 1.41
12.	Have Access To Data Models	2.7064	2.9725	- 2.26*
13.	Have Timesharing Training	3.2202	3.4679	- 2.77*
14.	Have Non-CBIS Audit Exprce.	2.9633	3.1568	- 2.38*
15.	Have Operating Systems Programming Experience	2.3486	2.5413	- 2.27*
16.	Have Data Base Systems Development Experience	2.3303	2.7431	- 3.98*
17.	Have Applications Systems Training	4.0183	4.0000	+ 0.23
18.	Have Non-CBIS Audit Training	3.5688	3.4679	+ 1.06
19.	Have Communications Technical Training	3.2569	4.0367	- 7.97
20.	Have On-line Programmer Experience	2.3303	2.6606	- 3.14
21.	Use Computing Tech. Specialists	4.1009	4.2936	- 2.48*
22.	Have long-Term Perspective	4.3119	4.3486	- 0.52
23.	Have Computer Operations Try	3.6330	3.4954	+ 1.58
24.	Have Distributed Data Processing Training	3.2385	4.1284	- 7.26*
25.	Have Distributed Data Process Experience	2.2844	3.0917	- 7.13
26.	Have Training in Info. Systems Mgmt.	4.0917	4.0092	+ 1.19
27.	Document Plan Before Doing	4.2936	4.3394	- 0.60
28.	Review Decisions With Non-CBIS Audit Staff	3.7431	3.8165	- 0.88
29.	Have Hardware/Software Monitors	3.1101	3.4120	- 3.44*
30.	Tailor Audit Objectives	4.1101	3.4120	- 0.48
31.	Have O.S. Training	3.5321	3.6881	- 1.76
32.	Have Technical Library	3.9450	4.2018	- 3.31*
33.	Have Comm. Analyst Exprce.	2.4128	3.0275	- 5.56*
34.	Use Tech. Specialists in Audit	4.0183	4.2752	- 3.63*
35.	Have Info. Systems Mgmt. Experience	2.8624	3.2294	- 5.17*
36.	Have Standard Audit Methods	4.1560	3.8899	+ 3.47*
37.	Have Software to Review System Usage	3.2752	3.3853	- 1.18

**Table 5.5**  
**CRITICALITY INDEX FOR SCENARIO A**

S.NO	COMPONENT	INDEX
1.	Review Audit Plan Relevance	.81
2.	Assure Proper Mix of Staff Skills	.73
3.	Tailor Audit Objectives	.72
4.	Document Plan Before Doing	.70
5.	Review Audit Plan Completeness	.69
6.	Use Computing Technical Specialists	.67
7.	Have Long Term Perspective	.61
8.	Have Standard Audit Methodologies	.59
9.	Use Technical Specialists In Audits	.59
10.	Have Training In Info. Systems Mgmt.	.58
11.	Use Participative Management	.56
12.	Have Applications Systems Training	.56
13.	Have Technical Library	.52
14.	Have Advanced Computer Training	.49
15.	Review Decisions With Non-CBIS Audit Staff	.47
16.	Use Communications Technical Specialists	.47
17.	Have Computer Operations Training	.44
18.	Have Operating System Training	.41
19.	Have Non-CBIS Audit Training	.41
20.	Have Distributed Data Processing Training	.32
21.	Have Software To Review System Usage	.30
22.	Have Advanced Non-CBIS Audit Training	.28
23.	Have Hardware/Software Monitors	.28
24.	Have Communications Technical Training	.23
25.	Have DBMS Training	.23
26.	Have Applications Development Experience	.21
27.	Have Non-CBIS Audit Experience	.18
28.	Have Timesharing Training	.18
29.	Have Advanced Communications Training	.17
30.	Have Information Systems Mgmt. Experience	.15
31.	Have Access To Data Models	.10
32.	Have Communications Analyst Experience	.06
33.	Have On-line Programmer Experience	.06
34.	Have Operating Systems Programmer Experience	.06
35.	Have Distributed Data Processing Experience	.05
36.	Have Data Base System Development Experience	.03
37.	Have Computer Operator Experience	.02

## **Criticality of Component Variables**

The criticality indices for the thirty seven (37) variables under Scenario A are shown in descending order in Table 5.5; those for the variables under Scenario B are shown in Table 5.6. These indices indicate the relative criticality of the factor components as expressed in the response data to items in the questionnaire.

Under Scenario A, thirteen (13) variables were judged to be critical to successful CBIS audit planning (having an index of 0.50 or greater); and under Scenario B, Seventeen (17) were so judged. All variables judged critical under Scenario A were also judged critical under Scenario B. In addition, four new variables under Scenario B were considered critical that were not critical under Scenario A. "Use Communications Technical Specialists" moved from sixteenth (with an index of 0.47) Under Scenario A to third (with an index of 0.81) under Scenario B. Similarly "Have Distributed Processing Training" moved from twentieth (20th) (at 0.32) to eleventh (at 0.63); "Have Communications Technical Training" from the twenty fourth (at 0.23) to twelfth (at 0.62); and "Have advanced Communications Training" from twenty ninth (at .17) to fifteenth (at .58). All of these deal with networking technology and their addition to the list of critical variables is clearly appropriate due to the increased networking emphasis of Scenario B.

Under Scenario B, there are more critical items to be included in planning a CBIS audit and the criticality, as indicated by respondents to the questionnaire, is generally higher than under Scenario A. For example, all seventeen (17) critical variables under Scenario B have equal or higher index values than the corresponding index values under Scenario A, with the exception of two variables.

The exceptions are 'Review Audit Plan Relevance' and "Have Standard Audit Methodologies". These are the same two components that were unusual in the analysis discussed in the previous section in which the results of the pair-wise t-tests were presented. They were the only components whose mean responses were statistically significantly higher under Scenario A than under Scenario B. The same reasoning as presented above regarding the generally higher availability of standard audit methods in Scenario A environments helps to explain the comparatively high importance placed upon these two component variables under Scenario A.

In order to assess whether the levels of criticality for variables recorded under Scenario A and B were significantly different, a pairwise t-test was performed on the index values. The mean of the indices under Scenario A was .3765 while that for Scenario B was .4568. The means were statistically significantly different at the 0.05 level, indicating that the thirty-seven (37) variables under consideration in this study are more critical during audit planning under Scenario B than under Scenario A. Once these preliminary analysis of the data collected were complete, it was necessary to determine the suitability of the data for use of factor analysis.

### **A p p r o p r i a t e n e s s   f o r   A n a l y s i s**

Several tests were conducted to assess the extent to which the factor analytic model could be considered appropriate for analysing the data collected during this research effort. The results of these tests were all favourable effectively eliminating the suggestion that the sample size of 109 respondents was inappropriately small for an application of factor analysis in this study.

For Example, the Kaiser-Meyer-Olkin (KMO) measure of overall sampling adequacy is an index for comparing the correlations between variables with their partial correlations. Small values for KMO indicate that the factor analysis may not be a good idea. For the Scenario A data, the KMO was .67327; for the Scenario B data the KMO was .72593. Both of these measures indicated that the use of factor analysis on the data structures was acceptable [Kaiser (1974)].

Additionally, measures of sampling adequacy (MSA Statistics) for each individual variable were constructed. Reasonably large values are needed for factor analysis. For Scenario A, the values ranged between .49305 and .79651; for Scenario B the values ranged between .46485 and .86840. These statistics indicated that none of the variables in the study were candidates for elimination from the analysis [Norusis (1986)].

The Bartlett test of sphericity was used to test the hypothesis that the correlation matrix for the population from which the sample data was drawn was an identity matrix. If the correlations between the variables are small, it is unlikely that they share common factors. The Bartlett test relies on a Chi-square Statistic, large values of which indicate rejection of the hypothesis. If the hypothesis that the population correlation matrix is an identity cannot be rejected, then the use of factor analysis should be reconsidered.

For Scenario A, the Bartlett statistic was 1958.916 which was statistically significant at the .05 level. For Scenario B the Bartlett statistic was also statistically significant at the .05 level as it was 2609.8921. Both hypotheses were, therefore, rejected indicating that the use of factor analytic techniques with the data collected in this research was appropriate.



Estimated correlations between factors and variables can be used to estimate correlations between variables. The structure of the resulting residuals between variables indicates how well the factor analysis model reproduces the observed correlations. For Scenario A, 30 percent of the residuals were greater than 0.05 and for Scenario B 26 percent. While there are no strict rules for residuals, statistics also indicate an acceptable fit.

### **Scenario A : Critical Success Factors**

A total of eleven factors were extracted from the Scenario A data using the principal components method of factor analysis and orthogonal rotation techniques under the varimax criterion, which minimises the number of variables within an analysis with higher factor loadings (In the orthogonal Case, these are the Correlations between the factors and variables). The rotation Converged in 24 iterations.

The communalities (that is, the amount of variance in an observed variable Component accounted for by the common factors) were high in the final rotated factor analytic solution for the Scenario A data. All exceeded .54 implying a high level of Common factor variance for each variable and that no variable should be removed from the factor analytic model in this case.

The eleven (11) critical success factors listed below were extracted from the Scenario A data using factor analysis.

Factor 1 - Computer Modeling Capability

Factor 2 - Information Technology Specialisation

Factor 3 - Computer/Networking Technical Training

- Factor 4 - Computer/Networking Technical Experience**
- Factor 5 - Advanced Technical Systems Experience**
- Factor 6 - CBIS Audit Engagement Management**
- Factor 7 - Traditional CBIS Audit Skills**
- Factor 8 - Traditional Financial Auditing Background**
- Factor 9 - Technical Reference Library**
- Factor 10 - Standardised Audit Methodologies**
- Factor 11 - Information Systems Management Training**

The Sequence numbers for the factors above are those that were assigned by the Computer software used to do the extraction. They have no significance in this analysis beyond that of an abbreviated label for the factors.

Each factor was developed by analysing the Component Variables that grouped together under that factor. Table 5.7 shows these groupings for the Scenario A factors. While all components with significant factor loadings (that is, with correlations above .30) were considered in the development of the composite variables (that represent the underlying common factors themselves), special consideration was given to those components with higher factor loadings. Factor scores (numerical estimates of the factors based upon linear combinations of the observed variables) were also included in Table 5.7.

Additionally, some factor loadings, perhaps comparatively small in absolute value, were nonetheless the largest for a given component. Therefore, each factor loading which had the largest magnitude for any one component was identified in Table 5.7 with a plus sign (+). This information was also utilised in constructing the factors.

**Table 5.6**  
**CRITICALITY INDEX FOR SCENARIO B**

S.NO	COMPONENT	INDEX
1.	Review Audit Plan For Completeness	.85
2.	Assure Proper Mix of Staff Skills	.85
3.	Use Communications Technical Specialists	.81
4.	Document Plan Before Doing	.74
5.	Tailor Audit Objectives	.73
6.	Review Audit Plan Relevance	.73
7.	Use Technical Specialists In Audits	.72
8.	Have Long Term Perspective	.72
9.	Use Computing Technical Specialists	.71
10.	Have Technical Library	.64
11.	Have Distributed Data Processing Training	.63
12.	Have Communications Technical Training	.62
13.	Use Participative Management	.62
14.	Have Applications Systems Training	.61
15.	Have Advanced Communications Training	.58
16.	Have Training In Info. Systems Management	.58
17.	Have Standard Audit Methodologies	.53
18.	Have Advanced Computer Training	.49
19.	Review Decisions With Non-CBIS Audit Staff	.48
20.	Have Software to Review System Usage	.38
21.	Have Operating Systems Training	.36
22.	Have Computer Operations Training	.36
23.	Have Timesharing Training	.33
24.	Have Hardware/Software Monitors	.33
25.	Have Info. Systems Management Experience	.31
26.	Have DBIS Training	.28
27.	Have Non-CBIS Audit Training	.26
28.	Have Distributed Data Processing Experience	.25
29.	Have Access To Data Models	.22
30.	Have Communications Analyst Experience	.21
31.	Have Advanced Non-CBIS Audit Training	.21
32.	Have Applications Development Experience	.20
33.	Have Non-CBIS Audit Experience	.20
34.	Have On-line Programmer Experience	.12
35.	Have Data Base Systems Programmer Experience	.06
36.	Have Operating Systems Programmer Experience	.05
37.	Have Computer Operator Experience	.00

Table 5.7

**FACTOR DETERMINATION FROM SCENARIO A**

**FACTOR 1 : COMPUTER MODELING CAPABILITY**

Factor Loadings	Factor Scores	Components
.80140 +	.31247	Have Hardware/Software Monitors
.74181 +	.25344	Have Access To Data Models
.72211 +	.26844	Have Software To Review Sys.
.49278 +	.11584	Have OP. SYS. Programming Exp.
.45710	.08092	Have D.B. Sys Devp. Experience
.43401 +	.09909	Have D.B.P. Experience
-.31154	-.19480	Have Adv. Computer Training
.30889	.01393	Have Technical Library
.30264	.03241	Have Communications Analyst Exp.

**FACTOR 2 : INFORMATION TECHNOLOGY EXPERIENCE**

Factor Loadings	Factor Scores	Components
.79267 +	.33298	Use Tech. Specialists In Audits
.78713 +	.32543	Use Computing Tech. Specialists
.70957 +	.33478	Assure Proper Mix of Staff Skill
.43653 +	.08606	Use Comm. Tech Specialists
.39614	.06286	Have Long Term Perspective
.39524	.12565	Document Plan Before Doing
.39262	.08610	Review Audit Plan Relevance
.30733	.09330	Have Comm. Analysts Experience

**FACTOR 3 : COMPUTER/NETWORKING TECHNICAL TRAINING**

Factor Loadings	Factor Scores	Components
.85352 +	.35922	Have Op. Systems Training
.78209 +	.31281	Have Computer Ops. Training
.52712 +	.19832	Have Comm. Tech. Training
.48091 +	.15172	Have Dist. Data Process. Traing.
.42133	.11192	Have Non-CBIS Audit Training
.40436	.14434	Have App. Systems Training
.30753	.02504	Have Training In Info. Sys. Mgm.

**FACTOR 4: COMPUTER NETWORKING TECHNICAL EXPERIENCE**

Factor Loadings	Factor Scores	Components
.77533 +	.39740	Have Op. Systems Training
.67805 +	.31167	Have Computer Ops. Training
.55628 +	.17443	Have Comm. Tech. Training
.52404 +	.21000	Have Dist. Data Process. Traing.
.50101 +	.11612	Have Non-CBIS Audit Training
.40450	.16581	Have App. Systems Training
.38328	.03006	Have Training In Info. Sys. Mgm.
.30891	.02794	Have Comm. Analyst Experience

**FACTOR 5 : ADVANCED TECHNICAL SYSTEMS EXPERTISE**

Factor Loadings	Factor Scores	Components
.80118 +	.37406	Have Adv. Comm. Trng.
.58660 +	.18190	Have Info. Sys. Mgmt Experience
.53856 +	.15540	Have Comm. Analyst Experience
.44244 +	.16867	Have Adv. Comp. Training
.43042	.20733	Have Dist. Data Process. Trg.
.40139	.10114	Have Dist. Data Process. Expce.
.38983	.16286	Use Comm. Tech. Specialists
.32963	.09719	Have Op. Sys. Program. Expce.
.31025	.04391	Have Data Base Sys. Devp. Expce.
.30690	.09056	Have Conun. Tech. Training
-.30363	-.20417	Have App. Syst. Training

**FACTOR 6 : CBIS AUDIT ENGAGEMENT MANAGEMENT**

Factor Loadings	Factor Scores	Components
.70016 +	.36434	Tailor Audit Objectives
.68847 +	.36601	Review Decision With Non-CBIS Audit Staff
.56771 +	.29118	Use Participative Management
.53916 +	.23289	Have Long Term Perspective
.34487	.16067	Review Audit Plan Completeness

**FACTOR 7: TRADITIONAL FINANCIAL AUDITING BACKGROUND**

Factor Loadings	Factor Scores	Components
.79905 +	.43358	Have Adv. Non-CBIS Audit Trg.
.69613 +	.32987	Have Non-CBIS Audit Experience
.54284 +	.21334	Have Non-CBIS Audit Training
.44699 +	.28008	Have Computer Operatios Exp.
.30436	.09512	Have Timesharing Training

**FACTOR 8 : TRADITIONAL CBIS AUDIT SKILLS**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.75558 + .68149 + .54260 + .47286 + .31677	.43571 .39804 .26595 .22154 .17256	Have DBMSTraining Review Audit Plan Completeness Have Appl.Sys. Training Review Audit Plan Relevance Document Plan Before Doing

**FACTOR 9 : TECHNICAL REFERENCE LIBRARY**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.70668 + .41910 .41150 -.40199 -.32182 .31291	.41236 .20326 .17036 -.26767 -.25271 .14215	Have Tech. Library Have DDP Training Have DDP Experience Document Plan Before Doing Have Computer Operator Expce. Have Appl.Sys. Training

**FACTOR 10 : STANDARDISED AUDIT METHODOLOGIES**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.88822 + .48101 +	.67571 .25153	Have Standard Audit Methods Review Audit Plan Relevance

**FACTOR 11 : INFORMATION SYSTEMS  
MANAGEMENT TRAINING**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.65433 + .35314 -.34093 -.33124 .31726	.44402 .21140 -.23460 -.19719 .20491	Have Training In Info.Sys.Mgm. Have Adv. Comp. Training Have Op. Sys. Progr. Experience Have DB Sys. Devp. Experience Use Participative Mgmt.

Each of the factors extracted from Scenario A is presented in the following pages. These discussions focus upon the categorisation of the components that grouped during the factor analysis process. This categorisation yielded a set of higher-order variables that represented the actual factors that were mathematically extracted from the data. The category labels, then, describe the critical success factors of this study.

### **Factor 1 - Computer Modeling Capability**

Nine components loaded onto this Scenario A factor as shown in Table 5.7. The top three factor loadings by far were for the components, "Have Hardware/Software monitors", "Have Access to Data Models", and "Have software to Review system usage". Furthermore, the factor loadings for these three components were the highest loadings onto any factor in the Scenario A analysis. These facts suggested the construct "Computer Modeling Capability."

Among the other six components loaded onto this factor, four dealt with a wide range of computing systems experience and one dealt with access to a technical library. All of these were consistent with the construct of "Computer Modelling Capability." That the component "Have Advanced Computer Training" was negatively loaded onto this factor seemed curious. However, it may have indicated a preference for technical experience over technical training as a basis for doing computer Modeling, which would be entirely plausible and consistent with the construct identified for this factor.

## **Factor 2 - Information Technology Specification**

Eight (8) components loaded onto this Scenario A factor. The four (4) components with the higher factor loadings were "Use Technical Specialist In Audit" "Use Computing Technical Specialists," "Assure the proper mix of staff skills," and "Use Communications Technical Specialists." Furthermore, the loadings onto this factor were the highest loadings onto any factor under Scenario A for these four (4) components. All of these considerations indicated the factor construct "Information Technology Specialisation."

Among the remaining four components that loaded onto this factor, "Review Audit Plan Relevance" and "Document Plan Before Doing" were consistent with the construct "Information Technology Specialisation," as was "Have Long Term Perspective." All of these components dealt, at a minimum, with managing the technological aspects of CBIS audit engagements including Planning.

Finally, the lowest factor loading included in this deliberation was for the component "Have Communications Analyst Experience." at .30733. This particular component did not appear to belong with the other components that loaded onto this factor; however, it was reasonably consistent with the "Information Technology Specialisation" construct in that it represented an area of specialisation and its influence upon the factor was minor.

## **Factor 3 - Computer/Networking Technical Training**

All seven (7) of the components that loaded onto this Scenario A factor dealt with technical training. The four (4) with the highest factor loadings for this factor also



did not load more highly on any other factor in the Scenario A analysis. These were "Have Operating Systems Training," "Have Computer Operations Training," "Have Communications Technical Training," and "Have Distributed Data Processing Training." These facts indicated that a general categorisation of "Computer/Networking Technical Training" was representative of the underlying construct.

In addition, three (3) other components loaded onto this factor. They were "Have Applications Systems Training," "Have Training In Information Systems Management," and "have Non- CBIS audit Training." First two (2) of these components were obviously consistent with the construct. "Computer/Networking Technical Training," The third, though it did not deal with technical systems training directly, reflected the sense that training in conventional financial audit methodologies would be useful in the context of CBIS audit planning. This is reasonably consistent with the construct as defined above.

#### **Factor 4 - Computer/Networking Technical Experience**

Seven (7) components loaded onto this Scenario A factor, all but one of which related to technical system experience (see, Table 5.7). Three (3) of these components exhibited the highest loadings onto this factor of any factors in the Scenario A analysis. These were "Have applications Development Experience" and "Have on-line Programmer Experience", which had the two (2) highest factor loadings for this factor, and "Have Data-Base Systems Development Experience". Among the other components that loaded onto this factor were "Have Information Systems Management Experience", "Have computer operation Experience," "Have operating system Programming Experience", and "Have Communications

**Analyst Experience". All of these suggested that a construct of "Computer/Networking Technical Experience" was appropriate.**

The only seemingly odd component that loaded onto this factor was "Have Time-sharing Training" which achieved its highest loading under scenario A onto this factor. The fact that this occurrence may be reflection of a perception on the part of respondents that time-sharing is an important aspect of technical experience, but the availability of experienced time-sharing technicians is limited. At any rate, this component was dominated in the factor by the other components in the group.

#### **Factor 5 - Advanced Technical Systems Expertise**

Eleven (11) components loaded onto this Scenario A factor. The top four (4) of these, all of which loaded onto this factor more highly than onto any other factor in the Scenario A analysis, were "Have Advanced Communications Training", "Have Information Systems Management Experience", "Have Communications Analyst Experience", and "Have Advanced Computer Training". Others included "Have Distributed Data Processing Training", "Have Distributed Data Processing Experience", "Have Operating Systems Programming Experience," "Have Database Systems Development Experience", and "Have Communications Technical Training." The combination of experience and training implied by these components indicated that the common construct that underlay this factor was "Advanced Technical Expertise".

Two (2) other components that loaded onto this factor were "Use Communications Technical Specialists" and "Have Applications Systems Training". The first

of these was probably attributable to a general perception by respondents that, particularly in a Scenario A environment, auditing communications technology was not typically needed for a CBIS audit engagement and having expertise in this area was de-emphasised accordingly. This was apparently manifested by a tendency to delegate auditing of networks, at least the complex ones, to communications technical specialists.

The component "Have Applications Systems Training" would have fit perfectly with this construct ("Advanced Technical Systems Expertise") except that its factor loading which had the smallest magnitude of the loadings considered for this Scenario A factor, was negative. In other words, this component and factor was negatively correlated. This may have reflected a feeling by the respondents that this component was inherently a part of the basic skills for the CBIS auditor and was, therefore, fundamentally different from the advanced expertise construct that underlay this factor. At any rate this component was dominated by the others in the group that loaded to this factor; and the component's influence upon the factor was clearly minor.

#### **FACTOR 6 - CBIS Audit Engagement Management**

Five (5) components loaded strongly to this Scenario A factor. All but one of these components exhibited the highest factor loadings to this factor of any of the Scenario A factors extracted in this study. The five (5) were "Tailor Audit Objectives," "Review Decisions with Non-CBIS Audit staff" "Use Participative Management," "Have Long Term Perspective," and "Review Audit Plan Completeness." For the components and factor loadings the underlying common factor construct was deemed to be "CBIS Audit Engagement Management."

### **FACTOR - 7 Traditional Financial Auditing Background**

Five (5) components loaded onto this Scenario A factor and four (4) of the five (5) components loaded strongly, with the four (4) corresponding factor loadings being the highest for those components in the Scenario A data. These were "Have Advanced Non-CBIS Audit Training," "Have Non-CBIS Audit Experience", "Have Non-CBIS Audit Training," and 'Have computer operator Experience.' This was a prescription for the construct "Traditional Financial Auditing Background," "Have Computer Operator Experience" had the Weakest loading of these four (4) factor components; this loading may be associated with the increasingly routine use of micro computers as a tool by CBIS auditors.

The last of the components that loaded onto this factor was "Have Time-sharing Training." This was consistent with the construct "Traditional Financial Auditing Background" in that, training in time-sharing system is common as preparation for CBIS auditing staff arising from this typically less technical background.

### **FACTOR 8 - Traditional CBIS Audit Skills**

Five (5) components loaded onto this Scenario A factor. The three (3) of these components with the highest factor loadings onto this factor also individually loaded onto this factor more than onto any other factor under Scenario A. There were "Have Data Base Management Systems Training", "Review Audit Plan Completeness", and "Have Applications Systems Training". Also, loading onto this factor were "Review Audit Plan Relevance", and "Document Plan Before Doing". All of these components clearly related to the construct "Traditional CBIS Audit Skills".

## **FACTOR 9 - Technical Reference Library**

Six (6) components loaded onto this Scenario A factor. These included the following three (3) components: "Have Technical Library", "Have Distributed Data Processing Training," and "Have Distributed Data Processing Experience". This factor was dominated by "Have Technical Library" both in terms of factor loading and factor scores. The influence of "Have Distributed Data Processing Training" and "Have Distributed Data Processing Experience". This factor was dominated by "Have Technical Library", both in terms of factor loading and factor scores. The influence of "Have Distributed Data Processing Training", and "Have Distributed Data Processing Experience" upon this factor were discounted since there was assumed to be no distributed data-processing within the Scenario A environment.

Two (2) other components had negative loadings onto this factor. One was "Have Computer Operator Experience". This kind of experience was simply not relevant to utilising the technical library function during an audit. The other was "Document Plan Before Doing". This apparently reflected a spurious correlation between this variable and the "Technical Reference Library" factor.

The last component that loaded onto this factor was "Have Applications Systems Training". This can be viewed as a minimum requirement to be able to use the technical system library function effectively during a CBIS audit engagement.

## **FACTOR 10 - Standardised Audit Methodologies**

Only two (2) components loaded onto this Scenario A factor; both factor loadings were the highest recorded for each of the two components for any factor evaluat-

ed under Scenario A. Infact, the factor loading for "Have Standard Audit Methods" which was .88822 was the highest correlation between a factor and a component alone, it was thus reasonable to postulate a construct "Standardised Audit Methodologies" for this factor.

The other factor component that loaded onto this factor was "Review Audit Plan Relevance". This component related to the construct in the sense that having standard Methodologies for CBIS auditing may have tended to limit the critical review of what was needed in an engagement. In other words, the auditor may have been prone to follow standard procedures whether they fit a given processing environment or not. Thus, "Review Audit Plan Relevance" was fully consistent with the construct "Standardised Audit Methodologies'.

#### **FACTOR 11 - Information Systems Management Training**

The last factor extracted under the Scenario A assumptions had five (5) components that loaded onto it. As with Factor 10, though to a lesser degree this factor was dominated by one key component, "Have Training In Information Systems Management" (See, Table 5.7). The appropriate construct was found to be "Information Systems Management Training."

"Have Advanced Computer Training" loaded onto this factor as well. This component probably represented the requisite level of technical education needed to be a candidate for the management training. Interestingly, both "Have Operating Systems Programmes Experience" and "Have Data Base Systems Development Experience" loaded negatively onto this factor, indicating that neither component contributed favourably to the construct "Information Systems

Management Training", at least as perceived by the respondents under Scenario A.

The last component to load (Somewhat, Minimally) onto this factor was "Participative Management". Certainly to the extent that technical specialists are becoming increasingly necessary to do various parts of CBIS Audit engagements, the use of participative management techniques must increase. Thus, it was not surprising that this component loaded onto this factor as it did.

### **Scenario B : Critical Success Factors**

A total of nine (9) factors were extracted from the Scenario B data using the principal components method of factor analysis with orthogonal rotation under the varimax criterion. The rotation converged in 18 iterations. The communalities for the final rotated Scenario B solution were comparable to those found for Scenario A above. All exceeded .52 implying a high level of common factor variance for each variable and that no variables should be removed from the factor analytic model in this case. The nine critical success factors extracted under the Scenario B assumptions are listed below :

Factor 1 - Computer/Networking Technical Experience

Factor 2 - Information Technology Specification

Factor 3 - Computer/Networking Technical Training

Factor 4 - Traditional Financial Auditing Background

Factor 5 - CBIS Audit Engagement Management

Factor 6 - Advanced Networking Expertise

Factor 7 - Standardised Audit Methodologies

Factor 8 - Audit Planning Flexibility

Factor 9 - Coordination with Financial Audit Staff.

As with Scenario A previously, the sequence numbers for the factors above are arbitrary. They have no significance beyond that of an abbreviated label for the factors.

Each factor was developed by analysing the component variables that grouped together under that factor. The Table 5.8 shows these groupings for the Scenario B factors. All components with Scenario B factor loadings (those above .30) were considered in the development of the factors; and, as with Scenario A previously, special consideration was given to those components with higher factor loadings. Both factor loadings and factor scores for the included components are shown in Table 5.8. Each of the factors extracted for Scenario B is explained in the following pages.

#### **Factor 1 - Computer/Networking Technical Experience**

Eleven (11) components loaded onto this Scenario B factor. The Seven (7) components with the highest loadings for this factor also posted the highest individual loadings for each of the seven (7) components under the Scenario B analysis. All of these seven (7) highest components dealt with technical expertise that was fully consistent with the construct defined above. The last dealt with time-sharing training and did not appear to belong with others. It was included in Table 5.8 for consistency (since its loading was greater than .30).

#### **Factor 2 - Information Technology Specialisation**

Twelve (12) factor components loaded onto this Scenario B factor. For six (6) of these components, the loadings onto this factor were the highest compared with all other Scenario B factors in the analysis. The five (5) components with the



**Table 5.8**  
**FACTOR DETERMINATION FROM SCENARIO B**

**FACTOR 1 : COMPUTER/NETWORKING TECHNICAL EXPERIENCE**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.77662 +	.20861	Have Data Base Sys. Devp. Exp.
.75446 +	.24162	Have Comp. Operator Experience
.73634 +	.17352	Have Appl. Devp. Experience
.72888 +	.14878	Have Info. Sys. Mgmt. Exp.
.72466 +	.16030	Have Op. Sys. Progmn. Experience
.70309 +	.14276	Have On-line Progmn. Experience
.66521 +	.11741	Have DDP Experience
.56719	.06347	Have Comm. Analyst Experience
.42127	.05371	Have Software To Review Sys. Us.
.40075	.08468	Have Access To Data Models
.35771	.03209	Have Timesharing Training

**FACTOR 2 : INFORMATION TECHNOLOGY SPECIALISATION**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.86142 +	.25121	Have Comm. Tech. Specialisation
.85970 +	.27318	Use Tech. Specialists In Audit
.84266 +	.24222	Use Comp. Tech. Specialists
.76003 +	.17571	Assure Proper Mix of Staff Skill
.65666 +	.23211	Have Tech. Library
.47614	.04634	Review Audit Plan Completeness
.43974	.01526	Use Participative Management
.42908 +	.08111	Have Hardware/SW Monitors
.33643	.01628	Have SW To Review Sys. Usage
.32800	.02003	Have Long Term Perspective
.31893	.03510	Have Adv. Comm. Training
.30597	.07839	Have Comm. Tech. Training

**FACTOR 3 : COMPUTER/NETWORKING TECHNICAL TRAINING**

<b>Factor Loadings</b>	<b>Factor Scores</b>	<b>Components</b>
.78750 +	.21524	Have Adv. Comp. Training
.77483 +	.23354	Have Op. Sys. Training
.69687 +	.17815	Have Computer Operations Trg.
.66965 +	.18001	Have DBMS Training
.63583 +	.15879	Have Comm. Sys. Training
.61164 +	.15822	Have Comm. Tech. Training
.54708 +	.13403	Have Timesharing Training
.50550 +	.08087	Have DDP Training
.49391	.08948	Have Info. Sys. Mgmt. Training
.42402	.07627	Have Adv. Comm. Training
.30379	.02758	Have Standard Audit Methods

#### FACTOR 4 : TRADITIONAL FIN AUDIT BACKGROUND

Factor Loadings	Factor Scores	Components
.89070 +	.33124	Have Adv. Non-CBIS Audit Trg.
.87660 +	.33113	Have Non-CBIS Audit Experience
.82745 +	.29294	Have Non-CBIS Audit Training
.35247	.09645	Review Decisions With Non-CBIS Audit Staff
-.35207	-.09612	Have Comm. Sys. Training

#### FACTOR 5 : CBIS AUDIT ENGAGEMENT MANAGEMENT

Factor Loadings	Factor Scores	Components
.61869 +	.33758	Use Participative Management
.56795 +	.26786	Tailor Audit Objective
.55614	.28809	Have Appl. Systems Training
.50274 +	.22604	Review Audit Plan Completeness
.50110	.23576	Have Training In Info. Sys. Management
.34226	.14027	Have Long Term Perspective

#### FACTOR 6 : ADVANCED NETWORKING EXPERTISE

Factor Loadings	Factor Scores	Components
.68915 +	.36667	Have Comm. Analyst Experience
.51975 +	.23075	Have Adv. Comm. Training
.51165	.22919	Have DDP Experience
.48204	.24390	Have DDP Training
.42075	.19451	Have Comm. Tech. Training
.36627	.16056	Have Info. System Mgmt. Exp.

#### FACTOR 7 : STANDARDISED AUDIT METHODOLOGIES

Factor Loadings	Factor Scores	Components
.73376 +	.43547	Have Standard Audit Methods
.70090 +	.16501	Review Audit Plan Relevance
.48372 +	.27830	Have Access To Data Models
.35618 +	.15091	Have HW/SW Monitors

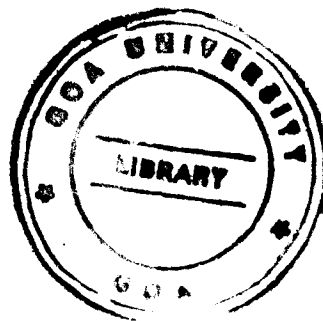
### FACTOR 8 : AUDIT PLANNING FLEXIBILITY

Factor Loadings	Factor Scores	Components
-.79472 +	-.50801	Document Plan Before Doing Have Software To Review Syst.Usage Have Timesharing Training
.48525 +	.28819	
.35471 +	.20600	

### FACTOR 9 : COORDINATION WITH FIN AUDIT STAFF

Factor Loadings	Factor Scores	Components
.62627 +	.44240	Have Long Term Perspective Review Decision With Non- CBIS Audit Staff Have HW/SW Monitors
.60912 +	.44103	
.34782	.22701	

U 424



highest factor loadings were "Use Communications Technical Specialists", "Use Technical Specialists in Audits", "Use computing Technical Specialists", "Assure Proper Mix of staff skills," and "Have Technical Library." All of these components suggested the construct "Information Technology Specialisation."

"Review Audit Plan Completeness" and "Use Participative Management" both were related to the technical specialisations construct in that more areas of technology were capable of being addressed with such specialisation, and staff specialities needed to be included in the management decision-making process within the context of increased specialisation, respectively. Also, the construct "Information Technology Specialisation," as it was extracted under Scenario B (and differing from the structure of this same factor as it was extracted under Scenario A) included system monitoring capabilities. This was exemplified by the loading of "Have Hardware/Software Monitors" and "Have Software To Review system usage" onto this factor. "Have Long Term Perspective" was another component that loaded onto this factor. Clearly, a longer perspective was appropriate within the context of a factor that focussed upon technical specialisation.

Curiously, the last two (2) components (with the lowest factor loadings considered for this Scenario B factor) were "Have Communications Technical Training" and "Have Advanced Communications Training". The fact that these two components loaded onto this particular factor may be representative of a perceived need among the respondents for training in communications in order to supplement the portfolio of specialisations needed CBIS auditing engagements in Scenario B environments.

### **Factor 3 - Computer/Networking Technical Training**

Eleven (11) components loaded onto this Scenario B factor. The first ten (10) of these dealt directly with technical training. "Have operating system Training," "Have computer operation Training," "Have Data Base Management systems Training", "Have Applications System Training", "Have Communications Technical Training", "Have Time-sharing Training," "Have Training In Information Systems Management," and "Have Advanced Communications Training." The first eight (8) of these components posted their highest loadings within the Scenario B analysis to this factor.

The eleventh component that loaded to this factor was "Have Standard Auditing Methods." This component was also related closely to the technical training factor and was consistent with this factor construct.

### **Factor 4 - Traditional Financial Auditing Background**

Five (5) components loaded onto this Scenario B factor. Four (4) with the highest factor loading (See, Table 5.8) were "Have Advanced Non CBIS Audit Training" "Have Non-CBIS Audit Experience," "Have Non-CBIS Audit Training," and "Review decision with Non-CBIS Audit Staff." All of these were consistent with an underlying factor "Traditional Financial Auditing Background." Furthermore, "Have Applications Development Experience" was negatively loaded onto this factor, which was entirely appropriate for this construct.

### **Factor 5 - CBIS Audit Engagement Management**

Six (6) components loaded to this Scenario B factor. four (4) of these six (6) components loaded more highly onto this factor than onto any other factors within the Scenario B analysis. Collectively under Scenario B, these six (6) components clearly shared a common factor, the construct for which was "CBIS Audit Engagement Management." These six (6) components were "Use Participative Management," "Tailor Audit Objectives," "Have Applications systems Training," "Review Audit Plan Completeness", "Have Training In Information Systems Management," and "Have Long-Term Perspective". The two training components were constructed to represent the basis of technical systems knowledge needed to manage such engagements.

### **Factor 6 - Advanced Networking Expertise**

Six (6) components were loaded onto this Scenario B factor. The five (5) with the highest factor loadings, all dealt with some aspect of networking technology. Also, the two components ("Have Communications Analyst Experience" and "Have Advanced Communications Training") loaded onto this factor more highly than onto any other Scenario B factor. Also, loading onto this factor were "Have Distributed Data Processing Experience", "Have Distributed Data Processing Training", "Have Communications Technical Training", and "Have Information Systems Management Experience". All of these were consistent with the construct "Advanced Networking expertise".

### **Factor 7 - Standardised Audit Methodologies**

Four (4) components loaded onto this Scenario B factor, three (3) of which exhibited the highest factor loadings onto this factor under Scenario B. By far the

highest loadings were for the two components "Have Standard Auditing Methods" and "Review Audit Plan Relevance". These suggested an underlying common factor of "Standardised Audit Methodologies". Also, loading onto this factor were "Have access to Data Models" and "Have Hardware/Software Monitors". The fact that those components loaded onto this factor probably reflected the perception of respondents that particularly under Scenario B assumptions, the factor "Standardised Audit Methodologies" needed to include automated tools for data collection as an integral part of such methodologies.

#### **FACTOR 8 - Audit Planning Flexibility**

Three (3) components loaded onto this Scenario B factor. Two (2) of the three (3) loaded more strongly onto this factor than onto any others within the Scenario B analysis. This was an unusual factor because it was strongly influenced by a component with a large negative factor loading. That loading was associated with the component "Document Plan Before Doing". Considering the inherent nature of the Scenario B environment, such a high negative loading for this component onto this factor was explained in terms of the need to be flexible in CBIS auditing situations with the Scenario B environment and its assumptions of technical complexity and diversity. Thus, the construct for this factor was "Audit Planning Flexibility." The perceived need for flexibility might also have derived partly from a lack of well established methods for auditing complex information technologies.

The other two components that loaded onto this factor were "Have software to Review Systems Usage" and "Have Time-sharing Training." Together these two

components were construed as indicating the need under Scenario B to have the tools and skills needed to maintain a flexible planning approach based, at least in part, upon system usage characteristics.

### **Factor 9 - Coordination With Financial Audit Staff**

Three (3) components loaded onto this Scenario B factor two (2) of which loaded more highly onto this factor than onto any others under Scenario B. The two components were "Have Long Term Perspective" and "Review Decision with Non-CBIS Audit Staffs". These components dominated the factor (see, Table 5.8) and they indicated that a factor analytic construct of "Coordination with financial Audit staff" was appropriate. Also loaded onto this factor was the component "Have Hardware/Software Monitors." The inclusion of this component in this factor probably reflected a perceived need among the respondents to have access to valid technical information regarding system characteristics and operation to facilitate coordination in a knowledgeable manner with financial audit staff. In the Scenario B environment, such access often requires technically sophisticated monitoring capabilities to collect such information accurately.

### **Criticality Measures For Factors**

In order to compare factors within and between Scenarios A and B, an overall index of criticality was constructed based upon the results of previous analysis performed during this research. That index was the "factor criticality index", and was simply the sum of the component criticality indices that loaded onto each factor (with a factor loading of .30 or greater). This index provided a relative



measure of the criticality of each factor within the context of the two basic scenarios undertaken. This measure was based upon the criticality scales in the data collection instrument, and therefore, the analysis of criticality were kept distinct from the factor analysis used to extract the factors. By separating the two parts of this analysis, two empirical basis were maintained for the two analytical foci of this research; first determining and then ranking the factors. The factor criticality indices, therefore, provided a relative measure of the degree of criticality for the critical success factors that were extracted under the Scenario A assumptions and those that were extracted under the Scenario B assumptions. It should be noted that these measures are only useful within each Scenario since the factor loadings are not necessarily comparable across different factor analysis, for example, those that were constructed in this study for the two different Scenarios. Table 5.9 through 5.19 show the results of this analysis for Scenario A; and Tables 5.20 through 5.28 depict the results for Scenario B.

In order to illustrate the use of these tables, consider factor 1 under Scenario B, "Computer/Networking Technical Expertise" (Table 5.20). This factor has a higher factor criticality index than "Standardised Audit Methodologies", "Audit Planning Flexibility", "Coordination with Financial Audit Staff", and "Traditional Financial Auditing Background". Yet none of the factor components that loaded on this factor had an individual criticality index higher than 0.50 while the other four mentioned did. The reason for this apparent inconsistency was the large numbers of components that loaded onto Factor 1. This obviously caused the factor index for this critical success factor to be higher, which was appropriate.

Another point of interest regarding Factor 1 of Scenario B was that the component "Have Computer Operations Experience" was very highly loaded onto this factor with a factor loading of .75446. It was the second highest component that loaded to this factor among a set of eleven (11) such components. However, since its individual criticality index was 0.00, this component had no influence on the value of the factor criticality index for the factor and would not be considered key in addressing this factor during CBIS audit planning exercises.

Table 5.9

**SCENARIO A FACTOR 1 CRITICALITY  
COMPUTER MODELING CAPABILITY**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.80140 +	.28	.2279	*HaveH/SMonitors (Sc. A, Question 28)
.74181 +	.10	.0742	*Have Access To Data Models (Sc. A, Question 12)
.72211 +	.30	.2166	Have Soft To Review Sys. Usage (A 37)
.49278 +	.06	.2957	*Have Op. Sys Prgrm. Exp (A 15)
.45710	.03	.0137	*Have Data Base Sys.Devp Experience 916)
.43401 +	.05	.0217	*Have DDP Exp. (A 25) -
.31154	.49	.1526	Have Adv. Comp. Trng. (A 7)
.30889	.52	.1606	*Have Tech. Library (A 32)
.30264	.06	.0181	*Have Comm. Analyst Exp. (A 33)
	1.89	0.9149	

**FACTOR CRITICALITY INDEX 1.89  
WEIGHTED AVERAGE COMP. INDEX 0.91**

Notes :- The absolute values of factor loadings were used to obtain cross products, "+" indicates the highest loadings given for that component; "\*" indicates significant difference between Scenario A and B data at the .05 level.

**Table 5.10**

**SCENARIO A FACTOR 2 CRITICALITY  
INFORMATION TECHNOLOGY SPECIALISATION**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.79627 +	.59	.4697	*Use Tech. Specs. In Audits (See A; Quest. 34)
.78713 +	.67	.5273	*Use Comp. Tech. Specs. (A 21)
.70957 +	.73	.5179	Assure Proper Mix of Staff Skills (A 11)
.43653 +	.47	.2051	* Use Comm. Tech. Specs. (A 3)
.39614	.61	.2416	*Have long Term Perspective (A 22)
.39524	.70	.2766	* Documents Plan Before Doing (A 27)
.39262	.81	.3180	*Review Audit Plan Relevance (A 8)
.30733	.06	.0184	*Have Comm. Analyst Exp. (A 33)
	4.64	2.5746	

**FACTOR CRITICALITY INDEX 4.64**

**WEIGHTED AVERAGE COMPOSITE INDEX 2.57**

Notes :- The absolute values of factor loadings were used to obtain cross products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenario A and B data at the .05 level.

**Table 5.11**

**SCENARIO A FACTOR 4 CRITICALITY**

**INFORMATION TECHNOLOGY SPECIALISATION**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.85352 +	.41	.3499	Have Op. Sys. Training (A 31)
.78209 +	.44	.3441	Have Comp. Ops. Trng. (A 23)
.52712 +	.23	.1212	* Have Comm. Tech. Training (A19)
.48091 +	.32	.1538	* Have DDP Trng. (A 24)
.42133	.41	.1727	Have Non-CBIS Audit Training (A 18)
.40436	.56	.2264	Have Appl. Sys. Training (A 17)
.30753 .	.58	.1783	Have Trng. In Info. Sys. Mgmt. (A 26)
	2.95	1.5464	

**FACTOR CRITICALITY INDEX 2.95**

**WEIGHTED AVERAGE COMPOSITE INDEX 1.55**

Note :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenario A and B data at the .05 level.

Table 5.12

SCENARIO A FACTOR 4 CRITICALITY

COMPUTER/NETWORKING TECHNICAL EXPERIENCE

Factor Loadings	Composite Criticality Index	Cross Product	Components
.77533 +	.21	.1628	Have Apptl. Devp. Exp. (A 10)
.67805 +	.06	.0406	*Have On-line Progr. Exp. (A 20)
.55628 +	.15	.0834	*Have Info. Sys. Mgmt. Exp. (A 35)
.52404 +	.18	.0943	*Have Timesharing Trg. (A 13)
.50101 +	.03	.0150	*Have DB Sys. Devp. Exp. (A 16)
.40450	.02	.0080	*Have Comp. Opr. Exp. (A 5)
.38328	.06	.0229	*Have Op. Sys. Progr. Exp. (A 15)
.30891	.06	.0185	*Have Comm. Analyst Exp. (A 33)
	0.77	0.4455	

FACTOR CRITICALITY INDEX 0.77

WEIGHTED AVERAGE COMPOSITE INDEX 0.77

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.13**

**SCENARIO A FACTOR 5 CRITICALITY**

**ADVANCED TECHNICAL SYSTEMS EXPERTISE**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.80118 +	.21	.1628	Have Apptl. Devp. Exp. (A 10)
.58660 +	.06	.0406	*Have On-line Progmr. Exp. (A 20)
.53856 +	.15	.0834	*Have Info. Sys. Mgmt. Exp. (A 35)
.44244 +	.18	.0943	*Have Timesharing Trg. (A 13)
.43042	.03	.0150	*Have DB Sys. Devp. Exp. (A 16)
.40139	.02	.0080	*Have Comp. Opr. Exp. (A 5)
.38983	.06	.0229	*Have Op. Sys. Progr. Exp. (A 15)
.32963	.06	.0185	*Have Comm. Analyst Exp. (A 33)
.31025	.03	.0093	*Have DB Sys. Devp. Exp. (A 16)
.30690	.23	.0705	*Have Comm. Tech. Trng. (A 19)
-.30363	.56	.1700	*Have Appl. Sys. Trng. (A 17)
	2.03	1.0835	

**FACTOR CRITICALITY INDEX 2.03**

**WEIGHTED AVERAGE COMPOSITE INDEX 1.08**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and Scenario B data at the .05 level.

**Table 5.14**

**SCENARIO A FACTOR 6 CRITICALITY  
CBIS AUDIT ENGAGEMENT PLANNING**

<b>Factor Loadings</b>	<b>Composite Criticality Index</b>	<b>Cross Product</b>	<b>Components</b>
.70016 +	.72	.5041	Tailor Audit Objectives (A 20)
.68847 +	.47	.3335	Review Decision With Non-CBIS Audit Staff (A 29)
.56771 +	.56	.3179	Use Participative Mgmt. (A 2)
.53916 +	.61	.3288	Have Long Term Perspective (A 22)
.34487	.69	.2379	Review Audit Plan Completeness (A 6)
	3.05	1.7122	

**FACTOR CRITICALITY INDEX 3.05**

**WEIGHTED AVERAGE COMPOSITE INDEX 1.71**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.



Table 5.15

SCENARIO A FACTOR 7 CRITICALITY

TRADITIONAL FINANCIAL AUDITING BACKGROUND

Factor Loadings	Composite Criticality Index	Cross Product	Components
.79905 +	.28	.2237	Have Adv. Non-CBIS Audit Trng. (A 4)
.69613 +	.18	.1253	*Have Non-CBIS Audit Exp. (A 14)
.54284 +	.41	.2225	Have Non-CBIS Audit Trng. (A 18)
.44699 +	.02	.0089	Have Comp. Operator Exp. (A 5)
.30436 +	.18	.0547	*Have Timesharing Trng. (A 13)
	1.07	0.6351	

FACTOR CRITICALITY INDEX 1.07

WEIGHTED AVERAGE COMPOSITE INDEX 0.64

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.17**

**SCENARIO A FACTOR 9 CRITICALITY**

**TECHNICAL REFERENCE LIBRARY**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.70668 +	.52	.3674	*Have Tech. Library (A 32)
.41910 +	.32	.1341	*Have DDP Trng. (A 24)
.41150 +	.05	.0205	*Have DDP Experience (A 25)
-.40199 +	.70	.2813	*Document Plan Before Doing (A 27)
-.32182 +	.02	.0064	Have Computer Opr. Exp. (A 5)
.31291	.56	.1752	Have Appl. Sys. Trng. (A 17)
	2.17	0.9849	

**FACTOR CRITICALITY INDEX 2.17**

**WEIGHTED AVERAGE COMPOSITE INDEX 0.98**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.18**

**SCENARIO A FACTOR 10 CRITICALITY**

**STANDARDISED AUDIT METHODOLOGIES**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.88822 +	.59	.5240	* Have Standard Audit Methods (A 36)
.48101 +	.81	.3896	* Review Audit Plan Relevance (A 8)
	1.40	0.9136	

**FACTOR CRITICALITY INDEX 1.40**

**WEIGHTED AVERAGE COMPOSITE INDEX 0.91**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.19**

**SCENARIO A FACTOR 11 CRITICALITY**

**INFORMATION SYSTEMS MANAGEMENT TRAINING**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.65433 +	.58	.3795	Have Training in Info. Sys. Mgmt. (A26)
.35314	.49	.1730	Have Adv. Computer Training (A-7)
.34093	.06	.0204	*Have Op. Sys. Progmr. Experience (A-15)
-.33124	.03	.0099	*Have Database Sys. Devp Exp. (A 16)
.30436	.18	.0547	Use Participative Management (A 2)
	1.72	0.7604	

**FACTOR CRITICALITY INDEX 1.72**  
**WEIGHTED AVERAGE COMPOSITE INDEX 0.76**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

Table 5.20

SCENARIO B FACTOR 1 CRITICALITY

COMPUTER/NETWORKING TECHNICAL EXPERIENCE

Factor Loadings	Composite Criticality Index	Cross Product	Components
.77662 +	.06	.0465	* Have Data Base Devp. Exp. (B-7)
.75446 +	.00	.0000	* Have Computer Ops. Exp.(B-24)
.73634 +	.20	.1472	Have App. Devp. Exp(B-31)
.72888 +	.31	.2259	* Have Info. Sys. Mgmt. Exp. (B-2)
.72466 +	.05	.0362	* Have OP. Sys. Progm. Exp. (B-35)
.70309 +	.12	.0843	* Have On-line Progm. Exp. (B-36)
.66521 +	.25	.1663	* Have DDP Exp. (B-28)
.56719	.21	.1191	* Have Comm. Analyst Exp.(B-16)
.42127	.38	.1600	Have Software to Rev. Sys. Usage (B-37)
.40075	.22	.0186	Have Access to Data Models (B-17)
.35771	.33	.1180	Have Timesharing Trng. (B-22)
	2.13	1.1221	

FACTOR CRITICALITY INDEX 2.13  
WEIGHTED AVERAGE COMPOSITE INDEX 1.12

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

Table 5.21

SCENARIO B FACTOR 2 CRITICALITY

INFORMATION TECHNOLOGY SPECIALISATION

Factor Loadings	Composite Criticality Index	Cross Product	Components
.86142 +	.81	.6977	* Have Comm. Tech. Specs. (B-10)
.85970 +	.72	.6189	* Use Tech. Specs. in (B-13)
.84266 +	.71	.5982	* Use Comp. Tech. Specs. (B-23)
.76003 +	.85	.6460	Assure Proper Mix of Staff -Skills (B-33)
.65666	.64	.4202	* Have Technical Library Complet. (B-1)
.47614	.85	.4047	* Rev. Audit Plan Complet (B-1)
.43974	.62	.2726	Use Participative Mgmt. (B-20)
.42908 +	.33	.1415	* Have HW/SW Monitors (B-9)
.33643	.38	.1278	Have Software To Reviews Sys. Usage (B-37)
.32800	.72	.2361	Have Long Term Perspective (B-32)
.31893	.58	.1849	* Have Adv. Comm. Trng. (B-15)
.30597	.62	.1897	* Have Comm. Tech. Trng. (B-3)
	7.83	4.5383	

FACTOR CRITICALITY INDEX 7.83

WEIGHTED AVERAGE COMPOSITE INDEX 4.54

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

Table 5.22

**SCENARIO B FACTOR 2 CRITICALITY**

**COMPUTER/NETWORKING TECHNICAL TRAINING**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.78750 +	.49	.385	Have Adv. Comp. Trng. (B-8)
.77483 +	.36	.2789	Have OP Sys. Training (B-11)
.69687 +	.36	.2508	* Have Comp. Ops. Trng. (B-34)
.66965 +	.28	.1875	* Have DBMS Trng (B25)
.63583 +	.61	.3878	Have Appl. Sys. Trng. (B-19)
.61164 +	.62	.3792	* Have Comm. Tech. Trng. (B-3)
.54708 +	.33	.1805	* Have Timesharing Trng. (B-22)
.50550 +	.63	.3184	* Have DDP Training (B-27)
.49391	.58	.2864	Have Training in Info. Sys. Mgmt. (B-14)
.42402	.58	.2459	* Have Adv. Comm. Trng. (B-15)
.30379	.53	.1610	* Have Standard Audit Methods (B-6)
	5.37	3.0622	

**FACTOR CRITICALITY INDEX 5.37**

**WEIGHTED AVERAGE COMPOSITE INDEX 3.06**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.23**

**SCENARIO B FACTOR 4 CRITICALITY**

**TRADITIONAL FINANCIAL AUDITING BACKGROUND**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.89070 +	.21	.1870	Have Adv. Non-CBSI Audit Trng. (B-12)
.87660 +	.20	.1753	*Have Non-CBIS Audit Expr. (B-5)
.82745 +	.26	.2151	Have Non-CBIS Audit (B-29)
.35247	.48	.1691	Review Decisions with Non-CBIS Audit Staff (B-26)
-.35207 -	.20	.0704	Have Appl. Develop Exper. (B-31)
	1.35	0.8169	

**FACTOR CRITICALITY INDEX 1.35**

**WEIGHTED AVERAGE COMPOSITE INDEX 0.82**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.



**Table 5.24**

**SCENARIO B FACTOR 5 CRITICALITY**

**CBIS AUDIT ENGAGEMENT MANAGEMENT**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.61869 +	.62	.3825	Use Participative Management (B-20)
.56795 +	.73	.4146	Tailor Audit Objectives (B-21)
.55614	.61	.3392	Have Appl. Sys. Trng. (B-19)
.50274 +	.85	.4273	*Review Audit Plan Comp. (B-1)
.50110 +	.58	.2906	Have Trng. in Info. Sys. Management (B-14)
.34226	.72	.2464	*Have Long Term Perspective. (B-32)
	4.11	2.1016	

**FACTOR CRITICALITY INDEX 4.11**

**WEIGHTED AVERAGE COMPOSITE INDEX 2.10**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.25**

**SCENARIO B FACTOR 6 CRITICALITY  
ADVANCED NETWORKING EXPERTISE**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.68915 +	.21	.1447	*HaveComm. AnalystExpe. (B 16)
.51975 +	.58	.3014	*HaveAdv. Comm. Trng. (B 15)
.51165	.25	.1279	* Have DDP Exper. (B 28)
.48204 +	.63	.3036	*HaveDDPTrng. (B27)
.42075 +	.62	.2608	*HaveComm. Tech. Trng. (B 3)
.36627 -	.31	.1135	* Have Info. Sys. Mgmt. Expe. (B 2)
	2.60	1.2519	

**FACTOR CRITICALITY INDEX 2.60**

**WEIGHTED AVERAGE COMPOSITE INDEX 1.25**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.26**

**SCENARIO B FACTOR 7 CRITICALITY  
STANDARDISED AUDIT METHODOLOGY**

<b>Factor Loadings</b>	<b>Composite Criticality Index</b>	<b>Cross Product</b>	<b>Components</b>
.73376 +	.53	.3888	Have Standard Audit Methods (B6)
.70090 +	.73	.5116	Review Audit Plan Relevance (B30)
.48372 +	.22	.1064	Have Access to Data Models (B17)
.35618	.33	.1175	Have HW/SW Monitors (B9)
-	1.81	1.1243	

**FACTOR CRITICALITY INDEX 1.81**

**WEIGHTED AVERAGE COMPOSITION INDEX 1.12**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.27**

**SCENARIO B FACTOR 8 CRITICALITY**

**AUDIT PLANNING FLEXIBILITY**

<b>Factor Loadings</b>	<b>Composite Criticality Index</b>	<b>Cross Product</b>	<b>Components</b>
<b>-.79472 +</b>	<b>.74</b>	<b>.5880</b>	<b>Document Plan Before Doing (B18)</b>
<b>.48525 +</b>	<b>.38</b>	<b>.1843</b>	<b>Have Software To Rev. Sys. Usage (B37)</b>
<b>.35471</b>	<b>.33</b>	<b>.1170</b>	<b>*Have Timesharing Trng. (B22)</b>
	<b>1.45</b>	<b>0.8893</b>	

**FACTOR CRITICALITY INDEX 1.45**

**WEIGHTED AVERAGE COMPOSITE INDEX 0.89**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

**Table 5.28**

**SCENARIO B FACTOR 9 CRITICALITY**

**CO-ORDINATION WITH FINANCIAL AUDIT STAFF**

Factor Loadings	Composite Criticality Index	Cross Product	Components
.62627 +	.72	.4508	Have Long-Term perspective (B32)
.60912 +	.48	.2923	Review Decisions With Non CBIS Audit Staff (B26)
.34782	.33	.1147	*Have HW/SW Monitors (B9)
	1.53	0.8578	

**FACTOR CRITICALITY INDEX 1.5WEIGHTED AVERAGE  
COMPOSITE INDEX 0.86**

Notes :- The absolute values of factor loadings were used to obtain cross-products; "+" indicates the highest loading given for that component; "\*" indicates significant difference between Scenarios A and B data at the .05 level.

A third example regarding Factor 1 of Scenario B involves the component "Have Information Systems Management Experience". This component has the third highest criticality index under the fourth highest factor loading of all the components that loaded to this factor. Therefore, the influence of this component on this factor would merit careful consideration by the CBIS audit engagement planner.

### **Critical Success Factor Rankings**

Based upon the overall indices developed for each factor, it is possible to rank the critical success factors that were extracted using factor analysis. Tables 5.29 and 5.30 show the rankings for Scenario A data and for Scenario B data respectively. Each set of factors is listed in descending order based upon the associated factor criticality indices that were developed as described previously.

Several observations are noteworthy. For example, "Information Technology Specialisation" was ranked highest under both Scenarios, and both "Traditional Financial Auditing Background" and "Computer/Networking Technical Experience" included no components with a criticality index of 0.50 or higher under either Scenario A or B. Furthermore, they were the only factors for either Scenario for which none of the components were higher than 0.50 in criticality.

Some information previously included in Table 5.4 (Statistically significant differences between response means under Scenario A versus Scenario B) and table 5.8 (The highest factor loading for a given component) was also summarised on Tables 5.9 through 5.28. Furthermore, a "Scenario identifier" and "Questionnaire item number" were included after each component label on these tables. Tables

Table 5.29

SCENARIO A FACTOR RANKINGS

S.No.	FACTOR	FACTOR NUMBER	FACTOR CRI. IND	RANK
1.	Information Tech. Specialisation	02	4.64	1
2.	CBIS Audit Engag. Mgmt.	06	3.05	2
3.	Traditional CBIS Audit Skills	08	2.99	3
4.	Comp/Network Tech. Training	03	2.95	4
5.	Technical Reference Library	09	2.17	5
6.	Adv. Tech. Sys. Expertise	05	2.03	6
7.	Computer Modeling Capabilities	01	1.83	7
8.	Info. Sys. Mgmt. Training	11	1.72	8
9.	Standard Audit Methodologies	10	1.40	9
10.	Traditional Fin. Audit Background *	07	1.07	10
11.	Computer/Networking Tech. Expe*	04	0.77	11

\*\*\* Indicates factors having no components with a Critical Index above 0.50

Table 5.30

SCENARIO B FACTOR RANKINGS

S.No.	FACTOR	FACTOR NUMBER	FACTOR CRI.IND	RANK
1.	Information Tech. Specialisative	02	7.83	01
2.	Comp/Net. Tech. Train.	03	5.37	02
3.	CBIS Audit Engage. Mgmt.	05	4.11	03
4.	Advanced Net. Expertise	06	2.60	04
5.	Com/Networking Tech. Experience	01*	2.1	05
6.	Standardised Audit Methodologies	07	1.81	06
7.	Coordination With Fin. Audit Staff	09	1.53	07
8.	Audit Planning Flexibility	08	1.45	08
9.	Traditional Fin Audit. Background	04*	1.35	09

\* indicates factors having no components with a Critical Index above 0.50



5.9 through 5.28 provide a factor by factor summary of the results of this research.

In conjunction with Table 5.29 and 5.30 which presented the overall ranking of the factors within each Scenario, the results presented in Tables 5.9 through 5.28 are further reviewed and summarised in the text chapter of this thesis. That chapter titled "Discussions", presents the overall findings and conclusion of this research, as well as its limitations and implications for future research.

## **CHAPTER 6**

### **DISCUSSION OF FINDINGS**

In this concluding chapter of the thesis, all those results, shown in the preceding Chapter 5, are summarised and integrated. The discussion begins by relating the theoretical critical success factors (as explained in Chapter 4) to the empirically based critical success factors extracted during this doctoral research (and presented in Chapter 5) for both traditional centralised computing environments and complex distributed data processing environments with networking facility. Subsequently, both the sets of empirically based factors are compared and contrasted. In addition to this, directions for future research relating to this technology presented.

#### **S u m m a r y   o f   R e s u l t s**

Three different sets of critical success factors were examined during the course of development of this research effort for conducting CBIS audit engagement planning.

The first set of critical success factors was developed theoretically as a basis for constructing a questionnaire for collecting data to address these issues empirically. This theoretical factor development was based upon Chapter 2 and 3. These factors were, therefore, intended to represent a complete list of relevant variables structured into appropriate categories, and did not presuppose any particular information system processing environment.

The other two sets of critical success factors utilised the same variables developed for the theoretical factors. These critical success factors were based upon

conducting CBIS audit planning activities within two different types of information systems processing environments. One complete set of factors was developed for each environment. These processing environments were defined within this study as arche-types, as follows :

- \* Centralised, monolithic computing systems referred to as scenario A environment.
- \* Complex, networking-based distributed computing systems referred to as scenario B environment.

The overall objective of this research is to compare the theoretical critical success factors to the actual critical success factors represented in the previous chapter with the corresponding scenario B critical success factors. Therefore, after a discussion of the theoretical factor constructs, the two sets of empirically derived critical success factors are compared and contrasted in the following pages.

### **Theoretical Factor Constructs**

In chapter 4, seven(7) categories of variables were presented. These constituted hypothetical factors and component variables relating to the planning of CBIS audit engagements. These seven (7) hypothetical factors are listed below :

1. Understanding of CBIS audit requirements.
2. Breadth of training.
3. Depth of training.
4. Breadth of experience.
5. Depth of experience.
6. Availability of audit tools.
7. Quality of professional judgement.

The individual component variables associated with each of these hypothetical factors is presented in Table 4.2. As noted above these variables are identical to those comprising the factors extracted using factor analysis under scenario A and B. Consequently, the variable grouping provided a basis for comparing the theoretical critical success factors with those for each scenario.

For the theoretical factors, each variable is used only once in the seven categories; while in the empirical cases, a variable may appear as often as it was loaded successfully into the available factors by factor analysis. Therefore, the theoretical factors can be systematically compared to the observed factors through these variables. For example, "Factor4-Computer/Networking Technical Training" under scenario A is nearly identical, in terms of its factor components, with the theoretical factor "Breadth of Experience". In fact, the training and experience factors under both Scenario A and B are nearly identical to their theoretical factor counterparts. However, a few other such overlapping similarities are evident.

In general, the theoretical factor constructs were less complex than the critical success factor constructs resulting from factor analysis. For example, Scenario A's "Factor2- Information Technology specialisation" was a mixture of "Depth of Experience" and "Quality of Professional Judgement" with a little "Understanding of CBIS Audit requirements" included. For Scenario B, this same factor is a mixture of the same theoretical factors as for scenario A, except that under this scenario "Availability of Audit Tools" is also included.

**Table 6.1**  
**COMPARISON OF SCENARIO A FACTORS WITH**  
**THEORETICAL FACTOR CONSTRUCTS**  
**[SCENARIO A]**

<b>Factor 1 - Computer Modeling Capability</b>	
Availability of Audit Tools	(4)
Breadth of Experience	(3)
Depth of Training	(1)
<b>Factor 2 - Information Technology Specialisation</b>	
Depth of Experience	(3)
Quality of Professional Judgement	(3)
Understanding of CBIS Audit Requirements	(2)
<b>Factor 3 - Computer/Networking Technical Training</b>	
Breadth of Training	(7)
<b>Factor 4 - Computer/Networking Technical Experience</b>	
Breadth of Experience	(8)
<b>Factor 5 - Advanced Technical Systems Expertise</b>	
Breadth of Experience	(5)
Breadth of Training	(3)
Depth of Training	(2)
Depth of Experience	(1)

**Factor 6 - EDP Audit Engagement Management**

Quality of Professional Judgement (3)

Understanding of CBIS Audit Requirements (2)

**Factor 7 - Traditional Financial Auditing Background**

Breadth of Experience (2)

Breadth of Training (2)

Depth of Training (1)

**Factor 8 - Traditional EDP Audit Skills**

Understanding of CBIS Audit Requirements (3)

Breadth of Training (2)

**Factor 9 - Technical Reference Library**

Breadth of Experience (2)

Breadth of Training (2)

Availability of Audit Tools (1)

Understanding of CBIS Audit Requirements (1)

**Factor 10 - Standardised Audit Methodologies**

Availability of Audit Tools (1)

Understanding of CBIS Audit Requirements (1)

**Factor 11 - Information Systems Management Training**

Breadth of Experience (2)

Breadth of Training (1)

Depth of training	(1)
Quality of Professional Judgement	(1)

NOTE :- Following each theoretical factor is a number in parentheses. That is the number of component variables that the indicated Scenario A factor had in common with the theoretical factor.

**Table 6.2**  
**COMPARISON OF SCENARIO A FACTORS WITH**  
**THEORETICAL FACTOR CONSTRUCTS**  
**[SCENARIO B]**

**Factor 1 - Computer/Networking Technical Experience**

Breadth of Experience	(8)
Availability of Audit Tools	(2)
Breadth of Training	(1)

**Factor 2 - Information Technology Specialisation**

Depth of Experience	(3)
Quality of Professional Judgement	(3)
Availability of Audit Tools	(3)
Breadth of Training	(2)

**Factor 3 - Computer/Networking Technical Training**

Breadth of Training	(9)
Depth of Training	(1)
Availability of Audit Tools	(1)

**Factor 4 - Traditional Financial Auditing Background**

Breadth of Experience	(2)
Quality of Professional Judgement	(1)
Depth of Training	(1)
Breadth of Training	(1)

**Factor 5 - EDP/CBIS Audit Engagement Management**

Quality of Professional Judgement	(2)
Understanding of CBIS Audit Requirement	(2)
Breadth of Training	(2)

**Factor 6 - Advanced Networking Expertise**

Breadth of Experience	(3)
Breadth of Training	(3)

**Factor 7 - Standardised Audit Methodologies**

Availability of Audit Tools	(3)
Understanding of CBIS Audit Requirements	(1)

**Factor 8 - Audit Planning Flexibility**

Understanding of CBIS Audit Requirements	(1)
Availability of Audit Tools	(1)
Breadth of Training	(1)

**Factor 9 - Co-ordination with Financial Audit Staff**

Quality of Professional Judgement	(2)
Availability of Audit Tools	(1)



Note: Following each theoretical factor is a number in parentheses, That is the number of component variables that the Scenario B factor had in common with the theoretical factor.

This kind of examination can be made for all of the Scenario A and B factors in terms of combinations of the theoretical factor constructs. Table 6.1 and 6.2 summarise these interrelationships for scenario A and B respectively. It should be noted that these tables only present a simplified, if insightful, summary of these relationships noted. They do not take into account the factor loadings of components or their criticality. For a detailed examination of these issues within this context, the tables in chapter 5 should be consulted. Nonetheless, the relationships in Table 6.1 and 6.2 are interesting in that they provide a connection between the literature review and theoretical foundation for this study and the empirically-derived research findings that have resulted.

### **Comparison of Scenario A And Scenario B Factors**

Using factor analytic techniques, eleven (11) critical success factors were extracted under scenario A and nine (9) were extracted under Scenario B. Six (6) of the factors extracted for Scenario A and B were the same. Though these factors were not identical in terms of their factor components, the components and loading patterns were similar enough to infer that the underlying factors were the same. Table 6.3 summarises the factors and this relative ranking for both the Scenarios. Comparisons of rankings of the factors provide several interesting insights into the impact of the technological systems environment on the CBIS auditing process. For example, "Information Technology Specialisation" was the most critical factor under both the scenarios. Even under a traditional processing scenario, the

Table 6.3

SCENARIO A AND B CRITICAL SUCESS FACTORS

S.No.	SCENARIO A	S.No.	SCENARIO A
1.	Information Technology Specialisation	1.	Information Technology Specialisation
2.	CBIS Audit Engagement Planning	2.	Computer/Networking Technical Training
3.	Traditional CBIS Audit Skills	3.	CBIS Audit Engagement Management
4.	Computer/Network Technical Training	4.	Advanced Networking Expertise
5.	Technical Reference Library	5.	Computer/Networking Technical Expereince
6.	Advanced Technical System Expertise	6.	Standardised Audit Methodology
7.	Computer Modeling Capability	7.	Co-ordination with Financial Audit Staff
8.	Information Systems Management Training	8.	Audit Planning Flexibility
9.	Standardised Audit Methodologies	9.	Traditional Financial Auditing Background
10.	Traditional Financial Auditing Background *		-----
11.	Computer Networking Technical Expereince		-----

\*\*\* Indicates factors having no components with a Critical Index above 0.50

need for technological specialisation was well understood. Of course, under scenario B, this factor was characterised by a system monitoring dimension that did not exist under scenario A. However, the basic criticality of this factor in both situations was clearly indicated. Additionally, the factor "Traditional Financial Auditing Background" was uniformly low in the ranking for both scenarios A and B. It is interesting that the respondents did not view this factor as among the most critical for the success of the CBIS auditing as among the most critical factors for the success of a CBIS audit planning effort even though the theoretical foundation for CBIS auditing are grounded in principle of financial auditing. This result may be explained by the high percentage of respondents with "Mostly computing back-grounds" as indicated in Table 5.2.

Also, the factors related to communications technology under Scenario A were less pronounced than under Scenario B. Under the former, Computing and networking Components tended to group together into combined factors. There appeared to be little differentiation between the two technologies in the minds of the respondents (under Scenario A assumptions). Under the latter, the networking components were more differentiated from computing components and "Advanced Networking Expertise" was ranked fourth. Of course, this is not too surprising given the basic technological emphasis of the two information processing Scenario, one being more Centralised and the other being more distributive.

There were six (6) common Critical success factors between the two Scenario. These six (6) Critical success factors are listed below with their relative ranking for each Scenario :

S.No. Common Critical Success Factor	Scenario	
	A	B
1. Information Tech. Specialisation	1	1
2. EDP Audit Engagement Mgmt..	2	3
3. Computer/Network Tech. Training	4	2
4. Standardised Audit Methodologies	9	6
5. Traditional Fin Audit. Background	10	9
6. Computer/Network. Tech. Experience	11	5

It is interesting that technical training is perceived to be highly critical to the success of a CBIS audit than technical experience and that standardised audit methodologies are perceived to be more critical than a background in financial auditing. Of course, audit engagement management is viewed as highly critical in both the environments. Among these common factors, with the exception of technical experience, the ordering of the factors within each Scenario was not dissimilar.

Perhaps, the deepest insights derived from this comparison relate not to the common factors between the two Scenarios but to the unique ones. Under Scenario A, five (5) unique critical success factors were extracted. These are listed below with their ranking in parentheses :

TRADITIONAL EDP AUDIT SKILLS	(3)
TECHNICAL REFERENCE LIBRARY	(5)
ADVANCED TECH. SYSTEMS EXPERIENCE	(6)
COMPUTER MODELING CAPABILITY	(7)
INFORMATION SYSTEMS MGMT. TRAINING	(8)

Under Scenario B, three Unique critical success factors were extracted as follows :

ADVANCED NETWORKING EXPERTISE	(4)
COORDINATION WITH FINANCIAL AUDIT STAFF	(7)
AUDIT PLANNING FLEXIBILITY	(8)

The differences between these two sets of unique critical success factors for CBIS audit planning illustrate the fundamental change that is occurring with the CBIS audit processes as a result of changing information systems

technology and the trends toward utilising distributed processing systems environments.

For Scenario B, fewer critical success factors emerged than for Scenario A indicating that the issues in successfully auditing complex CBIS environments are more tightly focused upon facility with the technology itself than within the traditional environments'. Under Scenario A, the unique factors listed above deal essentially with following a traditional approach ( Traditional EDP Audit Skills ) supplemented with specific areas of specialisation support Expertise, "computer Modeling Capabilities," and "Information systems Management Training")Conversely, in a Scenario B environment, "Audit Plan Flexibility" and "Coordination with Financial Audit Staff" are unique critical success factors that imply both a lack of experience with newer technologies and a real need to deal differently with the audit process itself rather than just the content of the CBIS portion of an audit. As information technology becomes more prolific and more complex, the need for flexibility in planning will increase. Simultaneously, the growth in the use of computer and network technology as a primary for information analysis and handling throughout and between the organisations implies that an increasingly critical coordination issue is developing within the audit of a typical Scenario B processing situation. This issue relates to the specter of being potentially and increasingly unable to establish financial audit reliance in Scenario B environments without a material CBIS audit contribution in such engagements. This involvement in audit reliance implies a growing need for coordination in the Scenario B environment.

In the Scenario B analysis, most of the content-related areas of specialisation that surfaced separately in the Scenario A analysis were loaded onto the common factors described previously. This implies that a generally high level of technical understanding is required to plan an audit in the Scenario B environment. In addition to this, overall higher level of technical expertise among the common factors, "Advanced Networking Expertise" is the only area of specialisation extracted by the factor analysis under Scenario B. This factor completes the technical basis needed for effectively planning CBIS audits in Scenario B environment by elevating this relatively new, but increasingly critical, specialisation within the existing portfolio.

### **Implications of This Research**

The implications of this research are extensive. A full spectrum of critical success factors for CBIS auditing has been developed. From the practitioner's point of view, CBIS audit planners can utilise these findings to tailor CBIS audit engagements depending upon the degree of centralisation that is present. The lists of factors are also ranked to facilitate the development of CBIS audit plans by assisting the planner to address more critical issues first. The fact that the components of each factor in each archetypical situation is available and also ranked according to criticality should facilitate CBIS audit planning all the more.

From the academician's point of view, a systematic framework for understanding and communicating the issues that lead to success/failure of CBIS audits has been proposed and tested. It should have value as pedagogical tool for instructing future CBIS auditors. Such instruction could occur within a formal education or professional training setting as needed.

From the researcher's point of view a research paradigm has been synthesised, theoretically supported, preliminarily examined, and offered for further investigation. The application of factors analytic techniques to determining critical success factors is a research contribution in its own right. Finally, the research itself provides important insights into the evolution of the CBIS auditing process as the underlying information technology matures.

Additionally, in a profession of generalists (CBIS auditors), the clear call coming out of this research is for technological specialisation. The development and management of such human resources is potentially a complex task with serious organisational implications. Sophisticated technical specialists can be difficult to motivate, control and utilise effectively. Yet, the need appears unavoidable within the context of CBIS auditing as information technology becomes increasingly diverse, distributed, and complex.

The changing critical success factors for CBIS auditing implies that the roles of CBIS auditors must change, shifting toward mandatory requirements for mastery of a wide range of technical knowledge. As computers and networks proliferate, the demarcation between financial auditing and CBIS auditing must necessarily shift towards increasing technical competency requirements for both CBIS and financial auditors. The implications, particularly for hiring of technically qualified candidate to do auditing and for providing adequate professional level CBIS training, are far reaching.

Technological evolution could also affect the highly critical area of CBIS audit engagement management by making it more difficult to manage such engage-



ments. The technical skills mix on CBIS audit engagements will increasingly become more key as technology becomes more diverse and complex. CBIS auditors with specialised skills will be more in demand for engagements whenever their specific skills match client's technological requirements. The combination of these roles and technological specialisation issues can be expected to create additional staffing and scheduling concerns that must be addressed.

Finally, there are potentially serious CBIS audit methodological implications. Increasing complexity and diversity of information technology during a time of increasingly rapid change in the technology itself, seriously hampers the ability to develop standard CBIS audit methodologies quick enough to be useful before they are obsolete or that fit more than a few situations. Yet, the development of standard methodologies is highly desirable as one key approach to routinising the various repetitive aspects of developing a detailed CBIS audit plan. On the one hand, having standard CBIS auditing methodologies is critical to the success of a CBIS audit planning process; while, on the other hand developing and effectively maintaining such methodologies is becoming increasingly more difficult.

These implications collectively place a premium on acquiring and nurturing a core of technical specialists who can deal successfully with the technological complexity, diversity and change primarily on the basis of superior knowledge. The professional and organisational implications of this kind of staffing are not insignificant. It is clear that such specialisation will have a broad impact on the CBIS auditor and the CBIS auditing profession.

## **Limitations And Future Research Directions**

The objectives of this research effort are achieved summarised subsequently. The critical success factors for conducting CBIS audit engagements planning in traditional centralised computing environments were identified. Similarly, the critical success factors for conducting planning in complex networking distributed computing environments were identified. The relative criticality of factors and components within each of these sets of critical success factors was identified. Using these factors as a basis of comparison, several conclusions were drawn regarding the impact of certain trends on CBIS audit planning. These are the current trends toward increasing complexity of information systems technology, particularly in the areas relating to communications networking.

This research effort was constrained by a lack of prior systematic empirical research (as explained in chapter 2) investigating the topic of CBIS auditing. The lack of a body of basic knowledge in this area mandated the theoretical and exploratory approach undertaken in this thesis. This approach inherently means that further research is needed to validate and solidify the results of this study.

The subjects who participated in this research were all external auditors and consultants. A natural extension of this research design would have been to collect the same data from internal auditors who engage in CBIS auditing and compare their audit planning perceptions to those of external auditors.

Furthermore, groups of external auditors in other organisations may hold differing opinions about the critical factors influencing CBIS auditing in different technical environments. Such differences of opinion could relate to differences in

hiring or training policies employed in other organisations. Thus, additional study of other external auditing organisations may be desirable.

The data collected for this study relied upon the self-reported perceptions of the respondents. While the research subjects probably perceived and reported their experiences and opinions accurately there is potential threat to the validity of the study inherent in such data collection procedures. It would have been more desirable to have obtained unobtrusive measures from the firms to validate certain of the responses received in an effort to strengthen the validity of the data collection. For example, it would have been especially helpful to have independent summary information regarding professional experience of respondents in CBIS audits while employed by the subject firm. However, such measures were not readily available.

The data was collected using an unvalidated questionnaire. Though the questionnaire items were based solidly on literature review and the theoretical foundation for this thesis, it was not possible to statistically validate this questionnaire prior to conducting the study. Consequently, the data collection instrument used could be incomplete or misleading in areas that could compromise the results of this research.

Each of these concerns provides a basis for further research into this topic. Statistical validation of the questionnaire, extension of the study to include additional external auditors from other organisations in this research, extension to include a Cross-Section of internal auditors in the study, and use of unobtrusive measures to validate self-reported responses, all represent opportunities for future research

into the topic of CBIS audit planning. The expansion and replication of this current research study with additional research subjects would be desirable.

Furthermore, the theoretical model presented in Chapter 3 of this thesis encompasses the entire process of CBIS auditing. It is not limited to engagement planning activity as was the empirical study that was done for this thesis. Figure 3.8 shows a theoretical framework upon which a wide range of research activity relating to this study could be established. This framework suggests a number of potential research questions dealing with CBIS auditing issues.

For example, the adequacy of specific CBIS audit procedures the basic issues of computer and network security, the auditability of complex information technology, the minimum requirements for and audit trail in large distributed systems environment, the relationships between professional judgement and training or professional judgement and experience, and the perception of clients of external auditors regarding audit effectiveness are potential topics of future research efforts that would be related to the current investigation. Others could include the relationship between CBIS audit requirements and CBIS audit procedures performed, the operating and performance requirements for effective CBIS audit tools in a variety of situations, and the impact of CBIS auditing activities on financial auditing activities with regard to audit reliance.

## **S u m m a r y   A n d   C o n c l u s i o n s**

This research has explored the impact of changing information technology on CBIS audit planning. In doing so, the critical success factors for planning CBIS audits in traditional centralised computing environments were compared and

contrasted with the critical success factors for planning CBIS audits in complex networking and distributed computing environments.

On Consolidation of critical factors, an increased emphasis upon higher understanding of the technology by auditors in general in the complex environments, and a marked reliance upon technical specialisation in auditing in both processing environments were found. Furthermore, six (6) common critical success factors encountered within both of the two processing environments were identified as well as subtle differences between these common factors across environments. Additionally, two sets of unique critical success factors were extracted from the data, one for each different processing environment. These critical success factors provided additional insights into the fundamental differences in CBIS audit planning for traditional centralised computing situations versus that for complex networking distributed computing situations.

And lastly, this has been exploratory research, as such, it may have raised more questions than it has answered. However, this effort represents a systematic beginning. As a result, this research has provided several significant insights into the process of planning for CBIS auditing engagements in a changing, increasingly complex, and increasingly diversified technological milieu.

## **BIBLIOGRAPHY**

**Ackoff, Russel L. (1970), A Concept of Corporate Planning, Wiley-Interscience : New York, John Wiley & Sons, pp. 9-18.**

**ACM (1985), Proceedings : IX Data Communication Symposium, IEEE - Computer Society Press : Washington D.C., pp 139 - 149.**

**AICPA (1978), Codification of Statements On Auditing Standards No. 1 to 21, American Institute of Certified Public Accountants : New York, pp. 83-93.**

**AICPA (1976) Statement of Auditing Standards No. 1. Sec. 320.28; American Institute of Certified Public Accountants : New York, pp. 21-23.**

**AICPA (1977) The Auditor's Study And Evaluation Of Internal Control in EDP Systems, American Institute of Certified Public Accountants :New York, pp. 18-63.**

**Albert L. Lederer & Jayesh Prasad (1992) "Better Cost Estimating", Communications of ACM, Vol. 35, No 2, pp. 51-59.**

**Allen, Brandt (1968) "Danger Ahead : Safeguard your Computer", Harvard Business Review, Vol. 46, No. 6 (Nov/Dec), pp. 97-101.**

**Allen, Brandt (1982), "An Unmanaged Computer System Can Stop you", Harvard Business Review, Vol. 60, No. 6 (Nov/Dec.), pp. 77-87.**

**Allen, Dennis (1992), "Sending A Message to Congress", BYTE, Vol.17, No.3, pp.10.**

**Amoroso, D. (1986) Effectiveness of End-User Developed Applications In Organisations : An Empirical Investigation(Unpublished Ph. D. Thesis), University of Georgia.**

**Andreychuk, M & Duffy, J. (1987), " The effects of office Automation, " COMPUTER JOURNAL, Vol. 30, No. 5 (Oct), pp. 30-33.**

**ANSCIPS (1982) American National Dictionary For Information Processing Systems, Technical Report X3/TR-1- 82, Computer & Business Equipment Manufacturers Association (USA).**

**Anthony, Robert N. (1965) Planning And Control System, A Framework For Analysis, A Framework For Analysis, Division of Research, Graduate School of Business Administration, Harvard University : Boston, pp. 17-28.**

**Anthony, Robert N. (1965), Dearden, John & Vancil, Richard F. (1972), "Key Economic Variables", Management Control Systems, Richard D. Irwin, Inc., Homewood - Illinois, pp. 147 - 158.**

**Arthur Anderson & Co. (1978), A Guide For Studying And Evaluating Internal Accounting Controls, Arthur Andersen & Co : Chicago, pp. 129-139.**

**Auramaki E, Hirschheim, R. & Lyytinen, K. (1992) "Modelling Offices Through Discourse Analysis : The SAMPO Approach," The Computer Journal, Vol. 35, No. 4, pp. 342- 352.**

**Avison, D.E. & Wood-Harper, A.T. (1991) "Information Systems Development Research : An Exploration of Ideas In Practice", The Computer Journal, Vol. 34, No. 2 (April), pp. 98-112.**

**Avison D.E., Fitzgerald G., Wood-Harper A.T. (1988) "Information Systems Development : A Tool Kit Is Not Enough", The Computer Journal, Vol. 31, No. 4, pp. 379.**

**Axner, David H. (1985), " Datacomm Test Equipment Diagnosis Network Performance", Telecommunication Products And Technology, (Aug), pp. 33-40.**

**Bailey, Andrew D. Jr. Gerlach, James & McAfee, R. Preston (1982), "An OSI Model For Internal Control Evaluation," ACM's SIGOA Newsletter, Vol. 3. No.1/2, pp. 27-28.**

**Baker, C.T. (1980), "Logical Distribution of applications & Data," IBM Systems Journal, Vol. 19, No.2, pp. 171-191.**

- Ball, L. & Harris R. (1982), "SMIS Members: A Membership Analysis," *MIS Quarterly*, Vol. 6, No.1, pp. 19-38.
- Barnes, Stanley H. et al (1978), "The Professionalism & the EDP Auditor," *The EDP Auditor*, (Winter), pp. 4-11.
- Beath, C.M. (1986) *Managing The User Relationship in Management Information Systems Projects: A Transaction Governance Approach*, (unpublished Ph.D Thesis), University of California, Los Angeles.
- Belitsos, Byron (1987), "Banking On WANs", *Communications International*, Vol. 14, No. 4, pp. 52-54.
- Bell, Daniel (1973) *The Coming of Post Industrial Society*, Basic Books: Newyork, pp. 28-33.
- Benbasat, Izak, Dexter, Albert S., Drury, Donald H. and Goldstein, Robert C. (1984), "A Critique of the Stage Hypothesis: Theory & Empirical Practice," *Communications of ACM*, Vol. 27, No.5, (May), pp. 466-475.
- Beguai, A. (1986), "Computer Crime: What can be Done About It?" *OFFICE*, Vol. 104, No.4 (Oct.) pp. 132.
- Bhat, Shrinivas & Harigopal, K. (1991), "States of Matter And Entropy Model For Crisis Management," *Research Bulletin/ICWAI*, Vol. X, No. 182, pp. 37-42.
- Bhattacharyya, G. & Mitra, s. (1991), "application Specific Networks: A Case Study," *Journal of Institution of Engineers (India) - Comp. Engineering Div.*, Vol. 71, (Sept.), pp. 32-41.
- Bostrom, Robert P. & Heinen, J, Stephen (1977 a), "MIS Problems & Failures: A Socio Technical Perspective -Part I", *MIS Quarterly*, Vol. 1, No.3, pp. 17-32.



- Bostrom, Robert P. & Heinen, J, Stephen (1977 b) , "MIS Problems & Failures: A Socio Technical Perspective Part II," *MIS Quarterly*, Vol. 1, No.4, pp. 11-28.
- Bradley, Layne C. (1985), "A Strategy For Network Planning and Control," *Journal of Information systems Management* Vol. 2, No.1 (Winter), pp. 21-28.
- Branscomb, L.M. (1979), "Computing & communications - a Perspective of the evolving environment," *IBM Systems Journal*, Vol. 18, No.2. pp. 189-201.
- Brill, Alan E. (1982), " EDP Auditors' Tales of Horror," *Journal of Systems Management*, (Jan.) pp. 20-22.
- Brown, Nander Jr. (1983), "Minicomputer Control, Security & audit," *The Internal Auditor*, (Feb.) pp. 39-42.
- Bruning, James L. & Kintz, B.I. (1977), *Computational Handbook of Statistics*, Scott, Foreman and Co. Glenview, Illinois (USA), pp. 13-28.
- Brooke, p.p., Russel, D.W., & Price, J.L. (1988)," Discriminant Validation of Measures of Job Satisfaction, Job Involvement and Organisational Commitment," *Journal of applied Psychology*, Vol. 73, No.2, pp. 139-145.
- Burg, Fred M., Chen, Cheng T., Folts, Harold C. (1984), "Of Local Networks, Protocols and the OSI refernce Model," *Data Communications*, (Nov.) pp. 129-150.
- Burnett, Gerald & Nolan, Richard L. (1975)," At Last, Major roles For Minicomputers," *Harvard Business review*, Vol. 53, No.3 (May/June) pp. 148-156.
- Burns, A.; Mc Dermid, J. Dobson, J. (1992), "On the Meaning of Safety & Security," *The Computer Journal*, Vol. 35, No.1, pp. 3-15.

Burton, F.W. (1987), "Functional Programming For Concurrent and Distributed Computing," *The Computer Journal*, Vol. 30, No.5 (Oct.) pp. 437-450.

Buss, Martin J. & Salerno, Lynn M. (1984), "Common Sense & Computer Security," *Harvard Business Review*, Vol. 62, No.2, pp. 112-121.

Camrass, Roger (1987), "New Technologies to make the Mark In Corporate Network," *Communication Systems Worldwide*, october, pp. 30-40.

Carlson, Arthur E. (1982), "Can Internal Accounting Control be Audited?", *Journal of Systems Management* (June), pp. 28-31.

Carol Wolinsky & James Sylvester (1992), "Privacy In The Telecommunication Age," *Communication of ACM*, Vol. 35, No. 2., pp. 23-25.

Chaffee, Dave (1987), "Major Challenges Ahead For Optical Communications," *Communication Systems Worldwide*, march, pp. 16-17.

Chakraborty, A., Chattopadhyay, P., & Mitra, S. (1990), "Information Protection & Computer Security In Banks: A Short Survey", *Journal of Institution of Engineers (India) - Computer Engineering Div.*, Vol. 71, (Sept.), pp. 32-41.

Cho, Y. (1986), "Implementation & Management of the Information Center : An Exploratory Study," (Unpublished Ph.D. Thesis), University of Nebraska, Lincoln. (USA).

Communication Systems Worldwide (1988), "India Updates with Local Switch," *Communication Systems*, February, pp. 9.

Communications Int. (1987), "Starting to Make Moves," *Communication International* , Vol. 14, No. 7, pp. 14.

- Daniel, D. Ronald (1961), "Management Information Crisis, " *Harvard Business Review*, Vol. 39, No. 5 pp. 28-30.
- Davis Charles K. & Wetherbe, James C. (1979), "An Analysis of the Impact of Distributed Data Processing on Organisations in the 1980's," *MIS Quarterly*, Vol. 3, No.4, pp. 47-56.
- Davis, Charles K. & Wetherbe, James C. (1980), "DSS For chargeout System Planning, Control in a Large-scale Environment, " *Data Base*, (summer) pp. 13-20.
- Davis, Charles K. & Wetherbe, James C. (1981), "Planning and Controlling Distributed Data Processing, " *Systems objectives And Solutions*, Vol.1, No.1, pp. 79-87.
- Davis, Gordon B. (1968), *Auditing & EDP*, AICPA: New York, pp. 29-49.
- Davis, Gordon B. (1974), *Management Information Systems: Conceptual Foundations, Structure and Development*, McGraw Hill: New York, pp. 192-98.
- Davis, Gordon B. Adams, Donald L. & Schaller, Carol A. (1983) *Auditing & EDP*, AICPA: New York, pp. 30-42.
- Davis, Gordon B., Weber, Ron (1983 a)," Auditing Advanced EDP Systems: A System Change Model, "In *Information Systems Auditing*, ed - by E.M. Wysong Jr. & Ivo Dellotto, Elsevier Science Publications : North - Holland, pp. 119-129.
- Davis, Gordan B. & Weber Ron (1983 b)," The Audit and Changing Information Systems", *The Internal Auditor*, (Aug.) pp. 34-38.
- Dean, Neal J. (1968)," The Computer Comes of Age," *Harvard Business Review*, Vol. 46, No. 7 (Jan./Feb.) pp. 83-91.

Dearden, John & Nolan, Richard L. (1973), "How to Control the Computer Resource," **Harvard Business Review**, Vol. 51, No.6, pp. 68-78.

Deen, S.M., Taylor M.C., Ingram P.A., Rayner K.W. (1988), "A Distributed Directory Database System For Telecommunication" **the Computer Journal**, Vpl. 31, No. 2 (April), pp. 175-101

Deloitte, Halkins, And Sells (1983), **EDP Management Controls Questionnaire - Draft**, Deloitte, Haskins & Sells: New York.

Deloitte, Halkins, And Sells (1985) **A Report For Congress And the Public**, Deloitte, Haskins & Sells: New York, pp. 19-49.

De Witt, D. & Gray, J (1992) " Parallel Database Systems : The Future of High Performance Data base Systems," **Communication of ACM** , Vol. 35, No. 6 (June), pp. 61-75.

Dickson, Gary W. Leitheiser, R.L. wetherbe, james C. and Nechis, Mal (1984)," Key Information Systems Issues For the 1980's," **MIS Quarterly**, Vol. 8, No.3, pp. 135-147.

Diebold, john (1985) **Managing Information - The Challenge And The Opportunity**, American Management Association: New York, pp. 38-79.

Dordick, H. Bradley, H.G., Nanus, B. & Martin, t. (1979) **The Emerging Network Marketplace**, Cambridge, Massachusetts Centre For Information System research, MIT, Working Paper.

Edpafer (1980) **Control Objectives 1980**, Altamonte Springs: Florida, EDP Auditors Foundation.

Elkins, Jeff (1985), " Status Reports Yield Key Data For Network Planning", **Data Communication**, (May) pp. 173-178.

Ernst & Whinney (1978) **Computer Controls Evaluation** Cleveland: Ernst & Whinney, pp. 21-31.

Fidlow, daniel (1985) "A Comprehensive Approach To Network Security," *Data Communication*, (April) pp. 195-210.

Finnie, Crahan (1985), "Mobile Data Takes to the Road," *Communications Systems Worldwide*, (March), pp. 22-23

Folger, robert a. & Sanderson, Glen R. (1983), "A Control Framework For Distributed computer systems," *The Internal Auditor*, (Oct.) pp. 71-78.

Freed, Roy N. (1969), "Get the Computer System You Want," *Harvard Business Review*, Vol. 47, No. 6 (Nov.-Dec.) pp. 99-108.

Frigon, Peter J. (1983), "Get as Much Tech control as You Need," *Data Communications*, Vol. (Oct.) pp. 167-173.

Fritchman, russel (1984), "security In Teleprocessing Networks," *EDP Journal*, Vol. 4, pp. 55-59.

Gallinger, george W. (1980), "Capital Expenditure Management," *Sloan Management Review*, Vol. 22, No. 1, pp. 13-21.

Gantz, John (1985), "Telecommunications Management: Who is incharge?" *Telecommunications Products & Technology* (Oct.) pp. 17-38.

Garrison, Willam J. (1984), "Designing The Computer & Communications Network Simulator," *Proceedings of the International Conference On The Management and Performance Evaluation of Computer Systems*, Sanfrancisco : The Computer Measurement Group. Inc.

Ghosh R, B. (1989), "AN Information Flow Model For Very Large Area Networks," *Journal of Institution of Engineers (Computer engineering Division)*, Vol. 70, No. (Sept), pp. 1-7.

Gibson, Cyrus F. & Nolan, Richard L. (1974), "Managing the Four Stages of EDP Growth," *Harvard Business Review*, Vol. 52, No.1, pp. 76-88.

Gillet, Bernard & Schwab, Donald P. (1975), "Convergent And Discriminant Validities of Corresponding Job Descriptive Index And Minnesota Satisfaction Questionnaire Scales," *Journal of Applied Psychology*, Vol. 60, No. 3, pp. 313-317.

Ginzberg, Michael J. (1981), " Key Recurrent Issues In The MIS Implementation Process," *MIS Quarterly*, Vol. 5, No. 2, pp 47-59.

Gitomer, Jerry (1985), "Achieving Optimum Main-Frame Performance with Front-End. Communications Processors," *Journal of Information System Management*, Vol. 2, No.1, pp. 57-62.

Gliezner, Schmel (1985), "The Dummy Entity, A Valuable Audit Tool," *The EDP Audit Control, And Security Newsletter*, Vol. XII, No. 12.

Gordon, Myron J. & Shillinglaw, Gordon (1969), *Accounting - A Management Approach* , Richard D. Irwin Inc. : Homewood, Illinois, pp. 112-14.

Green, P. E. (1979), " An Introduction to Network Architectures And Protocols," *IBM Systems Journal*, Vol. 18, No. 2, pp. 202-222.

Grehan, Rick (1990), " Some Assembly Required : Multitasking For The Masses," *BYTE*, Vol. 15, No. 2, pp. 279-288.

Gustafson, John R. (1975), " EDP Internal Auditing," *Information Systems Handbook* edited by Mc Farlan, F. Warren & Nolan, Richard L., Dow-Jones Irwin : Homewood, Illinois, pp. 192-205.

Guynes, Steve, Laney, Michael G. & Zant, Robert (1983), "Computer Security Practices," *Journal of Systems Management* (June), pp. 22-26.

Haldar, S. & Subramanian, D.K. (1989), " Load Balancing in Distributed Transaction Processing Systems," *Journal of Computer Science & Informatics*, Vol. 19, No. 2, pp. 1-12.

Hansen, James V. & Messier, William R. (1984), "A Relational Approach to Decision Support For EDP Auditing," *Communications of the ACM*, Vol. 27, No. 11, pp. 1129-1133.

Harman, Harry H. (1976) *Modern Factor Analysis*, Chicago : University of Chicago Press.

Harper, William L. & Pollard, Robert C. (1982) *Data Communication Desk Book : A Systems Analysis Approach*, Englewood Cliffs, New Jersey : Prentice - Hall Inc.

Helms, Glenn Lindley (1983) *An Examination Of The Impact Of Information Systems Auditor Involvement In Systems Development On The Quality Of New Application Systems*, Unpublished Ph. D. dissertation, University of Houston (through UMI Photo copy) pp. 247.

Helms, Glenn L. & Weiss, Ira (1983), " Auditor Involvement. In The Systems Development Life Cycle," *The Internal Auditor*, (Dec.) pp. 41-44.

Helms, Glenn L. & Weiss, Ira (1982), "Current Information Systems Auditor Involvement in Systems Developments : A Survey," *The EDP Auditor*, (Summer) pp. 13-20.

Herman, James (1987), "Connecting to WAN," *Communications International*, Vol. 14, No. 4, pp. 43-46.

Hiltz, Starr Roxanne And Turoff, Murrar (1978), *The Network Nation*, Reading, Massachusetts: Addison-Wesley Publishing Company.

Hirschheim R & Newman M. (1988), "Information Systems & User Resistance: Theory & Practice," *The Computer Journal*, Vol. 31, No.5, pp. 398-408.

Holland , Robert (1982), "Distributed Databases: Decisions And Implementation," *Data Communications* (May) pp. 97-111.

Holley, Charles L. & Miller, Frederick (1983), "Auditing the On-Line Real Time Computer Systems," *Journal of Systems Management*, (January), pp.14-19.

Holley, Charles L. & Reynolds, Keith (1984), "Audit Concerns in An On-Line Distributed Computer Network," *Journal of Systems Management*, (June), pp. 32-36.

Hooper, Paul & Page, John (1982), "Internal Control Problems in Computer Systems," *Journal of Systems Management*, (Dec.), pp. 22-27.

Horngrén, Charles T. (1982) *Cost Accounting: A Managerial Emphasis*, Englewood Cliffs, New Jersey: Prentice-Hall Inc.

Huck, Schuyler W., Cormier, William H., & Bounds William G. Jr. (1974) *Reading Statistics And Research*, New York: Harper & Row Publishers.

Hufnagel, E.M.(1987), "Information Systems Planning : Lessons from Strategic Planning," *INFORMATION MANAGEMENT*, Vol. 12, No. 5, (May), pp. 263-270.

Hull, M.E.C., O'Donoghue, P.G., Hagan, B.J. (1991) "Development Methods For Real Time Systems," *The Computer Journal*, Vol. 34, No. 2 (April) pp. 164-172.

IEEE (1984), *American National Standard : Local Area Networks - Logical Link Control*, New York: Institute of Electrical & Electronics Engineers Inc.

IEEE (1985 a), *American National Standard: Local Area Networks - carrier Sense Multiple Access With Collision Detection*, New York: Institute of Electrical & Electronics Engineers Inc.

IEEE (1985b), *American National Standard: Local Area Networks - Token Passing Bus Access Method*, New York: Institute Of Electrical & Electronic Engineers Inc.



IEEE (1985c), **American National Standard: Local Area Networks - Token Ring Access Method**, New York: Institute of Electrical & Electronic Engineers Inc.

Igbaria M., Greenhaus, J. H., Parsuraman, S. (1991), "Career Orientation of MIS Employees : An Empirical Analysis," *MIS Quarterly*, Vol. 15, No. 2 (June), pp.151-169.

Igbaria Magid & Jeffrey H. Greenhaus (1992), "Determinants of MIS Employees Turnover Intentions : A Structural Equation Model," *Communication of ACM*, Vol. 35, No. 2, pp. 35-49.

Institution of Engineers (India) (1989), **Management By Network Analysis**, Institution of Engineers (India) : Calcutta.

Jaikumar, V. M. & Gomez, Kevin (1986), "Banks Computerisation : Debit & Credit," *Computers Today*, (Jan.), pp. 25-33.

Jancura, Elise G. & Mechenzi, Alfred R. (1983), "Review of Distributed Data Base Systems," *The Internal Auditor*, (August), pp. 50-56.

Jarvenpaa, Sirkka L., Dickson, Gary W., & Desanctis, Gerardine (1985) "Methodological Issues In Experimental Is Research: Experience and Recommendations," *MIS Quarterly*, Vol. 9, No. 2, (June) pp. 141-156.

Jauhari, B. S. (1990), "Computer Based Electronic Office," *The Chartered Accountant*, (June), pp. 938-939.

Johnson, Joseph T (1985), "Universal Flow And Capacity Index Gives Picture of Network Efficiency," *Data Communication*, (Feb), pp. 171-173.

Johnson, Steve (1987), "SDN Alternative to Private Networks," *Communications engineering International*, Vol. 9, No. 2, pp. 55-59.

- Joyce, E.J. (1976), "Expert Judgement in Audit Programme Planning : Studies on Human Information Processing in Accounting," Supplement to Journal of Accounting Research, pp. 29-60.
- Joyce, Edward J. & Libby, Robert (1982), "Behavioural Studies of Audit Decision Making," Journal of Accounting Literature, Vol. 1, pp. 103-121.
- Jung, Kenneth G., Dalessio, Anthony & Johnson, S.M. (1986), "Stability of the Factor structure of the Job Descriptive Index," Academy of Management Journal, Vol. 29, No. 3, pp. 609-616.
- Kaiser, H.F. (1974), "An Index of Factorial Simplicity, Psychometrika, Vol. 39, pp. 31-36.
- Kaunitz, John & van Eckert, Louis (1984), "Audit Trail Compaction For Data-base Recovery," Communications of ACM, Vol. 27, No. 7. (July) pp. 678-683.
- Kay, R. (1986), "Computer Security Information Sources," COMPUTER SECURITY JOURNAL, Vol. 4, No. 1, pp. 21-28.
- Keplinger, H. & Davis, Charles K. (1983) "The Computer Pay Off," included in Strategies For Recovery In the Eighties, edited by Marvin E. Murphy, New York : The Oil Daily Energy Library, (October) pp. 225-240.
- Kerlinger, Fred N. (1973) Foundations of Behavioural Research, Holt, Rinehart & Winston Inc : New York.
- Kim, Jae-on & Muller, Charles W. (1978 a) Introduction To Factor Analysis, Sage Publications Inc : Beverley Hills (USA)
- Kim, Jae-on (1975), "Factor Analysis" Statistical Package For the Social Sciences, edited by N.H. Nie, C.H. Hull, J.G. Jenkins, K. Steinbrenner, & D.H. Bent, McGraw-Hill : New York, pp. 468-514.

**Kim, Jae-on & Muller, Charles W. (1978 b) Factor Analysis, Sage Publications Inc : Beverley Hills (USA).**

**Kimbel, D (1987), "Information Technology : Today & Tomorrow," TELECOMMUNICATIO POLICY, Vol. 11, No. 4 (Dec.), pp. 377-390.**

**King, John L. & Kraemer, Kenneth L. (1985), "Evolution and Organisational Information Systems : An Assessment of Nolan's Stage Model, "Communications of ACM, Vol. 27, No. 5 (May), pp. 476-485.**

**Kleinrock, Leonard (1985), "Distributed Systems," Communications of ACM, Vol. 28, No. 11 (Nov), pp. 1200-1213.**

**Kovach, Roger & Inselberg, Armond (1984), "Performance Software Ensures DP Efficiency," Data Management, (April), pp. 12-14.**

**Kriebel, Charles H. & Strong, Diane M. (1984), "A Survey of MIS and Telecommunications Activities In Major Business Firms, " MIS Quarterly, Vol. 8, No. 3, pp. 171-177.**

**Lampe, James C. & Kneer, Dan C. (1984), "Audit Implications Of Distributed Data Processing," EDP Journal, Vol. 3, pp. 39-50.**

**Lathrop, David M. (1985), "Auditors, Who Needs Them? "Journal Of Systems Management, (March), pp. 20-22.**

**Lecht, Charles (1977), Waves Of Change, Advanced Computer Techniques Corporation : New York.**

**Levin, David P. (1984), "Needs Assessment In Data Communications Network, "Journal of Information Systems Management, Vol. 1, No. 3, pp. 56-65.**

- Lientz, B.P. & Swanson, EB. (1980), "Impact Of Development Productivity Aids On Applications Systems Maintenance, 'Data Base, (Winter/Spring), pp. 114-120.
- Lientz, B.P. & Weiss, Ira (1978, "Trade Offs of Secure Processing In Centralised Versus Distributed Networks, "Computer Networks, Vol. 2, No. 1, pp. 35-43.
- Ling, D.H.O. & Bell, D. A. (1992), "Modelling & Managing Time in Database Systems," The Computer Journal, Vol. 35, No. 4, pp. 332-341.
- Litecky, Charles R. & Rittenberg, Lary E. (1981), "The External Auditor's Review Of Computer Controls,"Communications Of ACM, Vol. 24, No. 5, (May), pp. 288-295.
- Lockwood, D.L. & Sobol, M.G. (1989), "IS Spending Survey: Communications Technologies Dominate Growth Areas," Journal of Systems management, Vol. 40 (Dec.) pp. 31-37.
- Lord, Robert J. (1975), "Trends In Audit & IRS Practices And Their Implications For The Information Systems Manager, "The Information Systems Handbook, edited by F.W. McFarlan & R.L. Nolan, Dow Jones Irwin inc : Homewood, Illinois, pp. 176-191.
- Lorin, H. (1979), "Distributed Processing : An Assessment, "IBM Systems Journal, Vol. 18, No. 4, pp. 582-602.
- Lucas, Henry C. Jr. (1982), Information Systems Concepts For Management, Mc Graw-Hill Book Co. New York.
- Lucas, H. C. Jr. (1989), Managing Information Services Mac Millan - New York pp. 12-15.
- Lucas, Henry C. Jr. (1975), Why Information Systems Fail, Columbia University Press: New York.

**Lucas, Henry C. Jr. (1985), The Analysis, Design, and Implementation of Information Systems, Mc Graw-Hill Book company: New York.**

**Lundberg, olof (1988), " Moving Towards A Wireless Society," Communication Systems, (February), pp. 16-26.**

**Madnick, Stuart E. (1978), "Management Policies & Procedures Needed For Effective Computer Security", Sloan Management Review, Vol. 20, No. 1 (Fall).**

**Magid Igbaria & Jeffrey H. Greenhaus (1992), "Determinants of MIS Employees Turnover Intentions : A Structural Equation Model," Communication of ACM, Vol. 35, No. 2, pp. 35-49.**

**Mair, W. C., Davis, K. W. & Wood, D. R. (1972), Computer Audit & Control, The Institute of Internal Auditors. Inc: Altamonte Springs, Florida (USA).**

**Martin, E. W. (1982), Critical Success Factors of Chief MIS/DP Executives, "IS Quarterly, Vol.6, No. 2, pp. 1-9.**

**Martin, James (1981 a), Computer Networks & Distributed Processing, Prentice-Hall Inc: Englewood Cliffs New Jersey (USA)**

**Martin, James (1981 b), Telematic Society, Prentice-Hall Inc: Englewood Cliffs, New Jersey (USA).**

**Mason, John O: (1975), "Management Information System - The Auditor's Role, "The Internal Auditor, (Sept/Oct) pp. 40-48.**

**Mathias, James E. (1982), " Strategic Communications Management, "Journal of Systems Management, (Oct), pp 18-27.**

- McCanley, Herbert N. (1983), "Developing A Corporate Private Network, "MIS QUARTERLY, Vol. 7, No. 4 (Dec), pp. 19-33.
- McFarlan, R. Warren (1973), "Management Audit of EDP Department, "Harvard Business Review, Vol. 51, No. 3 (May/June), pp. 131-142.
- McFarlan, R. Warren, McKenny, James L., And Pybum, Philip (1983), " The Information Archipelago-Plotting A Course, "Harvard Business Review, Vol. 61, No. 1, (Jan/Feb), pp. 145-156.
- McInerney, Francis (1987), "Picking Winners In Switching," Communications Systems Worldwide, (February), pp. 42-44.
- McKenny, James L. & McFarlan, R. Warren (1982)", The Information Archipelago-Maps And Bridges, "Harvard Business Review, Vol. 60, No. 5 (Sept/Oct), pp. 109-119
- Menkus, Belden (1983), "Long-Haul Data Security : Whose Responsibility Is It Today? "Data Communication, (March), pp. 137-144.
- Menkus, Belden (1985), "Protecting Corporate Data, "Journal of Systems Management, (April), pp. 14-19.
- Merchant, K. A. (1985), Control In Business Organisations, Pitman Publishing Inc: Boston (USA).
- Mier, Edwin E. (1985), "Special Report-PBX Trends & Technology Update: Following The Leaders, "Data Communications, (Sept), pp. 02-96.
- Mintzberg, Henry (1976), "Planning On the Left Side & Managing on the Right, "Harvard Business Review, Vol. 54, No.4 pp. 54.

- Mitchell, Terence A. (1985), "An Evaluation of the Validity of Correlational Research Conducted in Organisations," *Academy of Management Review*, Vol. 10, No. 2 (April), pp. 192-205.
- Monger, Rodney (1981), *Issues, Characteristics, and Resolution Modes of Determinates of Conflict Between Auditor and Client*, Unpublished Ph.D. Dissertation (Micro) UMI- University of Houston.
- Morrison, Perry R (1983), "A Survey of Attitudes Toward Computers," *Communications of the ACM*, Vol. 26, No. 12, pp. 1051-1057.
- New Data Com, london (1988), "Encryption Algorithm Foils the Data Tapper," *Communications Systems World wide*, (April), pp. 12.
- Nolan, Richard R. (1982), "Managing Information Systems By Committee," *Harvard Business Review*, Vol. 60, No. 4 pp. 72-79.
- Nolan Richard R. (1979), "Managing the Crisis In Data Processing," *Harvard Business Review*, Vol. 57, No. 2, pp. 115-126.
- Nolan Richard R. (1973), "Plight of the EDP Manager", *Harvard Business Review*, Vol. 51, No. 3, pp. 143-152.
- Norris, Daniel M. (1983), "Judgement Characteristics of Minicomputer Auditors," *EDP Journal*, (Summer), pp.35-41.
- Norusis, Marija J. (1986), *Advanced Statistics: SPSS/PC+ For the IBM PC/XT/AT*, Chicago: SPSS Inc:(USA).
- Novotny, Eric J. (1979), "Restrictions On The Transnational Flow of Corporate Information : New Challenges For The Auditing Profession," *The EDP Auditor*, Summer, pp. 13-33.

- O'Neil, Jack (1985), "What to look for in a Network Monitoring And Control System," **Telecommunications Products And Technology**, (Aug), pp. 26-30.
- Paddock, Charles E. & Scamell, Richard W. (1984), "Office Automation Projects & Their Impact On Organisation, Planning, & Control," **ACM Transactions On Office Information Systems**, Vol. 2, No. 4 (Oct.), pp. 289-302.
- Padmanabhan, T. G. (1989), "Integrated Network Management & SCADA Systems," **Journal of Institution of Engineers (India) - Computer Eng. Div.**, Vol. 70, (Sept.) pp. 8-11.
- Parker, Donn B. (1981), **Computer Security Management**, Reston Publishing Company : Reston, Virginia.
- Parker, Donn B. (1983), **Fighting Computer Crime**, Scribner's : New York.
- Parker, Donn B. (1984), "Many Faces of Data Vulnerability," **IEEE Spectrum**, Vol. 21, No. 5 (May), pp. 46-49.
- Parker, Donn B. (1979), "Vulnerabilities of EFT's to Intentionally caused Losses," **Communications of the ACM**, Vol. 22, No. 12, pp. 654-659.
- Parker, Nycom, Susan H (1984), "Computer Crimes," **Communications of the ACM**, Vol. 27, No. 4, pp. 313-315.
- Parker, M. & Benson, R.J.(1987) "Information Economics : An Introduction," **DATAMATION**, Vol. 33, No. 23, (Dec.), pp. 86-100.
- Pathak, Jagdish P. (1990), "On Concurrent Auditing Of EDP : Flow Chart Algorithm," **The Chartered Accountant**, (June), pp. 932-944.



**Pathak, Jagdish P. (1991), "Management of MIS : A Challenge to Management Accounting Sphere," Research Bulletin/ICWAI, Vol. X, No. 1 & 2, pp. 23-27.**

**Pathak, Jagdish P. (1988), "Goal Oriented programme Efficiency Test In Operational EDP Audit : A Markovian Experiment," Research Bulletin/ICWAI, Vol. VII, No. 1 & 2, pp. 9-17.**

**Pearson, Ken (1989), "The Key to Flexible Data Networks," Communications Systems Worldwide, (Dec./Jan), pp. 44-47.**

**Perkins, James H. (1983), "planned Evolution Will Solve EDP Problems," The Internal Auditor, (Dec.), pp. 48-51.**

**Perry, Tekla S. & Wallich, Paul (1984), "Can Computer Crime Be Stopped? " IEEE Spectrum, Vol. 21, No.5, pp.35-45.**

**Perry, William E. (1983), Auditing Computer Programmes, EDP Auditors Foundation : Carol Stream, Illinois (USA).**

**Perry, William E. (1981), Auditing Data Systems, EDP Auditors Foundations : Carol Stream, Illinois (USA).**

**Perry, William E. (1983), Auditing Hardware & Software Contracts, EDP Auditors Foundation : Carol Stream, Illinois (USA).**

**Perry, William E. (1983), Auditing Information Systems, EDP Auditors Foundation : Carol Stream, Illinois (USA).**

**Perry, William E. (1983), Auditing the Small Business Systems, EDP Auditors Foundation : Carol Stream, Illinois (USA).**

- Perry, William E. (1981), **EDP Audit Work Papers**, EDP Auditors Foundation : Carol Stream, Illinois.
- Perry, William E. (1985), **Management Strategies For Computer Security**, Butterworth Publishers, Boston.
- Perry, William E. (1981), **Planning EDP Audits**, EDP Auditors Foundation : Carol Stream, Illinois (USA).
- Perry, William E. (1981), **Selecting EDP Audit Areas**, EDP Auditors Foundation : Carol Stream, Illinois (USA).
- Perry, William E. (1984), "The Relationship Between EDP Audit & Quality Assurance," **Journal Of Information Systems Management**, Vol. 1, No. 1, pp. 90-92.
- Perry, William E., Warner, Henry C. (1978), "Systems Auditability - Friend or Foe," **Journal Of Accountancy**, (Feb), pp. 52-60.
- Phister, Montgomery Jr. (1986), **Data Processing Technology And Economics**, Digital Press: Bedford, Massachusetts.
- Pipino, Leo L. (1978), "The Internal Auditor as Diagnostician in an EDP Environment," **The Internal Auditor**, (Feb.), pp. 03-00.
- Pitroda, Sam (1988), "India Confronts Tele-Com Future," **Communications Systems Worldwide**, (January), pp. 46.
- Poczek, Slobadon (1985), "Smart Monitoring Gives a new look at Network Vitals," **Data Communication** (May), pp. 199-203.
- Porter, W. Thomas & Perry, William E. (1984), **EDP Controls And Auditing**, Kent Publishing Co: Boston.

- Potter, D. (1987), "Long Range Systems Planning," *Datamation*, Val. 33, No. 10, (May), pp. 113-120.
- Raymond, L. (1987), "Information Systems Designs For Project Management," *Project Management Journal*, Vol. 18, No. 4, (Sept.), pp. 94-99.
- Read, Richard (1989), "Data Security - A Question of Control," *Communication Systems Worldwide*, (Feb.), pp. 42-45.
- Reel, Nanci & Hawranek, Joseph P. (1985), "The Preservation of Network Integrity & Encryption," *Telecommunication*, (May), pp. 76-04.
- Reuter, Vincent G. (1985), "Selected Management Controls: Audits, Budgets, and capital Funds Justification," *Journal of Systems Manangement*, (August), pp. 14-21.
- Rittenberg, Larry E. & Purdy, Charles R. (1970), "The Internal Auditors Role In MIS Development," *MIS Quarterly* (Dec), pp 47-57.
- Rittenberg, Larry E. & Davis, Gordon B. (1977), "The Role of Internal Auditors And External Auditors in Auditing EDP Systems," *Journal of Accountancy* (Dec.), pp. 51-58.
- Roberts, Ray (1978), "Impact On The Auditor of the Recent Developments Relating to Internal Control," *The EDP Auditor*, (Winter), pp. 12-20.
- Rockart, John F. (1978), *A New Approach to Defining the Chief Executive's Information Needs*, Centre For Information Systems Research-MIT: Cambridge.
- Rockart, John F. (1979), "Chief Executives Define Their Own Data Needs," *Harvard Business Review*, Vol. 57, No.2 (March/April), PP. 81-88.

Rushinek Avi & Rushinek, Sara F. (1984), "A User Evaluation of Information Characteristics related to demand Deposit Systems: An Empirical Analysis", **Information & Management**, Vol. 7, No.2, pp 69-72.

Russo, Paul M. (1983), "VLSI Impact on Micro-processor Evolution Usage and Systems Design", **Advanced Microprocessors**, edited by Gupta, Amar & Too-ong Hoo-min D:IEEE Press, New York, pp. 20-29.

Salsburg, Michael A. (1984), "Using Simulation: Major Network Decisions, "Proceedings of the international Conference on Management and Performance Evaluation of Computer System, Computer Measurement Group Inc: San Francisco (USA).

Sape Mullender (1991), **Distributed Systems ACM - Addison- Wesley**, New York, pp. 9-12.

Schneidman, Arnold (1979), "Need For Auditors' Computer education," **The CPA Journal**, (June), pp. 29-35.

Seid, Howard A. (1983), "The Ins And Outs of Managing a Packet Network," **Data Communications**, (October) pp. 149-161.

Shapiro, Ehud Y. (1983), "The V. Generation Project. A Trip Report," **Communications of the ACM**, Vol. 26, No. 9.

Singhal, A. & Rogers, E. M. (1989), **Information Revolution In India**, Sage Publications : New Delhi.

Smith, John H. & Uecher, Wilfred C. (1977), "Internal Audit Activities In EDP System Design, Testing, & Control," **The Internal Auditor**, (February), pp. 57-62.

Spooner, P. (1987), "Computers," **CHIEF EXECUTIVE**, (Sept.), pp.25-27.

Stallings, William (1984), "Local Networks," *Computing Surveys*, Vol. 16, No. 1 (March), pp. 3-41.

Stanford Research Institute (1977), *Systems Auditability & Control Study*, The Institute of Internal Auditors: Altamonte Springs; Florida (USA).

Stewart, H. M. (1979), "Performance Analysis of Complex Communications Systems," *IBM Systems Journal*, Vol. 10, No. 3, pp. 356-373.

Stix, G. (1987), "The High Cost of Global Reach," *COMPUTER COMMUNICATION DECISIONS*, Vol. 19, No. 11 pp. 52-53.

Swanson, E. B. (1982), "Critique of Ginzberg Article: Key Recurrent Issues in the Implementation Process", *MIS Quarterly*, Vol. 6, No.2 (Sept), pp. 73-74.

Swanson, E. B. (1976), "The Dimension of Maintenance", *Proceedings of the II International Conference on Software Engineering : Piscataway, New Jersey*, pp. 492- 497.

Synott, William R. & Gruber, William H (1981), *Information Resource Management*, John Wiley & Sons: New York.

Tanenbaum, Andrew S. (1981), *Computer Networks*, Prentice-Hall Inc: Englewood Cliffs-New Jersey.

Thierauf, Robert J. (1984), *Effective Management Information Systems*, Charles E. Merrill Publishing Co: Columbus (USA).

Thomas D. Clark Jr. (1992), "Corporate Systems Management," *Communication of ACM*, Vol. 35, no. 2 pp. 61-75.

Touche Ross & Co. (1979), *Controlling Assets And Transactions* Touch Ross & Co: New York.

Trotman, K. T. & Yetton, P. W. (1985), "The Effect of the Review Process on Auditor Judgements," *Journal of Accounting Research*, (Spring), pp. 20-25.

Urban, Glen L. & Hauser, John R. (1980), *Design and Marketing of New Products*, Prentice-Hall Inc:Engle wood Cliffs - New Jersey (USA).

Van Zutphen, L. C. (1980), "Developments In Computer Technology and the EDP Audit Function," *Audit Research in the Professional Firm*, AICPA: New York pp. 147-163.

Van Name, Mark L. & Catchings, Bill (1990a), "Networks :  
Hard Choice For Network Managers," *BYTE*, Vol. 15, No.12, pp. 97-106.

Van Name, Mark L. & Catchings, Bill (1990b), "Networks :  
A Natural Match," *BYTE*, Vol. 15, No. 6, pp. 109-112.

Venecek, Michael T., Soloman, Ira & Mannino, Michael V. (1983), "The Data Dictionary : An Evaluation for the EDP Audit perspective," *MIS Quarterly*, Vol.7, No. 1 (March), pp. 15-27.

Verrijin - stuart, A. (1970) "Themes & Trends In Information Systems : 1975-1985," *The Computer Journal* Vol. 30, No. 2, pp. 97-109.

Voydock, Victor L. & Kent, Stephen T. (1903), "Security Mechanisms in High-Level Network Protocols," *ACM Computing Surveys*, Vol. 15, No. 2 (June), pp. 135-171.

Wabler, Robert C. Jr. (1984), "Auditing For Efficiency in the on line systems," *EDP Journal*, Vol. 4 pp. 1-4.

Walko, John (1988a), "Switching On The Network," *Communications Systems Worldwide*, (June), pp. 44-47.

Walko, John (1988b), "Europe's Data Dilemma," *Communications Systems Worldwide*, (Sept.), pp. 5.

Walko, John (1987), "IDR Ready To Take Off," **Communications Systems Worldwide**, (Sept.), pp. 34.

Walsh, Myles E. (1984), "Telecommunications - A Reconciler of Incompatibilities," **Journal of Systems Management**, (Sept), pp. 12-23.

Ware, Willis H. (1984), "Information Systems Security & Privacy," **Communications of ACM**, Vol. 27. No. 4, pp. 315-321.

Wasserman, Joseph J. (1969), "Plugging the leaks in computer Security," **Harvard Business Review**, Vol. 47, No. 5, pp.119-129.

Weber, Ron (1984), **EDP Auditing - Conceptual Foundations and Practice**, McGraw-Hill Book Co: New York.

Weber, Ron (1980), "Some Characteristics of the Free recall of computer Controls by EDP Auditors," **Journal of Accounting Research**, Vol. 18, No.1, pp. 214-241.

Weiss, Ira R. (1980) "Auditability of Software: A Survey of Techniques & Costs," **MIS Quarterly**, Vol. 4, No. 4.

Weiss, Ira R. & Boockholdt, J. (1981), Complimentary EDP Audit Techniques, "The EDP Auditor," (Spring).

Westermeier, J. T. (1985), "Computer Crime Statutes: How do they affect Information Policy?" **Information Strategy: The Executive's Journal**, Vol.1, No. 3, pp. 40- 42.

Wetherbe, James C. (1979), **Systems Analysis For Computer Based Information Systems**, West Publishing Co: St. Paul, Minnesota (USA).

Wetherbe, James C., Davis, Charles K. & Dykman, Charlene A. (1981), "Implementing Automated Office Systems," **Journal of Systems Management**, Vol. 32, No. 8, pp. 6-11.

- Wilkinson, W. (1978), "Evaluating Controls in Advanced computer Systems, "Internal Auditor, (October).
- Williams, Davis J. & Lillis, Anne (1985), "EDP Audits of operating Systems - An Exploratory Study of Determinants of Prior Probabilities of Risk, "Auditing, Vol. 4, No. 2, pp. 110-117.
- Withington, F. G. (1987), "Managing Your Information Systems Pros.," Datamation, Vol. 33, No. 20 (Oct.), pp. 72-81.
- Withington, Fredrick G. (1980), "Coping With Computer Proliferation," Harvard Business Review, Vol. 58, No. 3, pp. 152-164.
- Witten, Ian H. (1983), "The New Microprocessors," Advanced Microprocessors, edited by Gupta, Amar et al, IEEE Press : New York, pp. 12-19.
- Wood, Charles C. (1984), "Countering Unauthorised Systems Access," Journal of Systems Management, (April), pp. 26-28.
- Woodburn, Valerie (1987), "PC Users Look For Connectivity," Communications Systems Worldwide, (July/Aug.), pp. 17-21.
- Wooding, Giles C. (1984), The Audit and Control of Real Time Distributed Database Systems, Unpublished DBA Thesis, George Washington University (through UMI-USA).
- Wysong, Earl M. Jr. (1983), "Using the Internal Auditor for systems Design Projects, "Journal Of Systems Management, (July), pp. 28-32.
- Yeager, Samuel J. (1981), "Dimensionality of the Job Descriptive Index," Academy of Management Journal, Vol. 24, No. 1, pp. 205-212.
- Young, L.F. (1987), "A Systems Architecture for Supporting Senior Managers' Messy Tasks,'Information Management, Vol. 13, No. 2, (Sept), pp. 85-94.



**CONFIDENTIAL USE**  
**ACADEMIC/RESEARCH ONLY**

Deptt. of Management Studies,  
GOA UNIVERSITY

21st March, 1991.

J. P. PATHAK  
Doctoral Research Fellow  
GOA UNIVERSITY  
BAMBOLIM  
(GOA)

Dear External Audit Specialist,

The enclosed questionnaire has been developed as the basis of a study that is concerned with the impact of increasing information systems complexity upon the information systems auditing process. You have been identified as an individual who participates in information systems audits in a variety of technological environments. For this reason, you are being requested to participate in this study. Your participation is completely voluntary and no adverse consequences will result if you decline to participate or subsequently withdraw.

The questionnaire should take about 30 minutes to complete. All questions relate solely to your understanding of and experiences in planning and conducting information systems audit engagements in traditional centralised information systems environments versus your experiences in complex distributed information systems environments. Please focus upon the two arche types described in the questionnaire and disregard in your answers any configurations that may be combinations of these two basic types of processing environments.

Your responses to the questions will be held in strictest confidence. No codes or other forms of identification are placed on the questionnaire that would enable anyone to determine which questionnaire you submitted. Only aggregate data will be published in the thesis. The results of this study will form the part of Ph.D. Dissertation at the Faculty of Management Studies, University of Goa.

In case you have any questions regarding this letter or the questionnaire, then please do not hesitate to contact me at my Panaji (Goa) residence at D-4-2; Govt. Officers' Flats, Altinho-Panaji 403 001 (Goa) or at my office phone No. (0832) 45973.

Sincerely

J.P. PATHAK

Enclosed : As above

### Instructions For Answering The Questionnaire

The Questionnaire includes questions in one of the three formats :

1. Most of the questions in this Questionnaire are statements that require responses on a scale that is numbered from 1 to 5. Put a circle around your response number.
2. Another form of question often used is the multiple choice format, in which the response would be to check mark the appropriate answers among those listed.
3. Third form of questions occasionally used in this Questionnaire is of the "fill-in-the-blank" type.

NOTE : After completing the Questionnaire, please enclose it in the attached self-addressed confidential envelope and mail it at your earliest convenience.

## INFORMATION SYSTEMS AUDIT PLANNING QUESTIONNAIRE

The following questions are designed to help evaluate the factors in planning information systems audit engagements that are critical to achieving a successful audit. A successful audit is one that is appropriate for the particular information systems environment and effective in terms of its specific technical content, the depth and breadth of the review done, and the materiality of the analyses performed from the business perspective of the organisation being audited.

The questionnaire consists of two similar parts. The first part deals with planning information systems audits in traditional, mostly centralised large scale computing environments. A hypothetical scenario designated "Scenario A" and describing such an environment is summarised below.

The second part deals with planning information systems audits in distributed, mostly decentralised large-scale networking environments with computing systems located at nodes of the network. A second hypothetical scenario, designated "Scenario B" and describing such an environment is also presented below.

**INFORMATION SYSTEMS AUDITORS**

Your participation in this research effort is appreciated. The following questions concern background information about your position, education and experience. This information will be used only for the analysis of group data and not for the identification of individuals. Please place check marks ( ) in the squares to the left of the appropriate answers and provide written information when requested.

1. Present Designation \_\_\_\_\_

2. Period spent with the firm \_\_\_\_\_ years and \_\_\_\_\_ months.

3. Period spent in Present Designation \_\_\_\_\_ years and \_\_\_\_\_ months.

4. Age \_\_\_\_\_

5. Sex \_\_\_\_\_

6. Approximate number of audits, you participated during

1980 - 85 \_\_\_\_\_ 1985 - 90 \_\_\_\_\_

1991 \_\_\_\_\_

7. Roles Performed in Audit engagements : (check all that apply).

Manager

Project Leader

Analyst

EDP Accounting Controls Specialist

EDP General Controls Specialist

EDP Application Controls Specialist

- EDP Administrative Controls Specialist
- Computing Technology Specialist
- Networking Technology Specialist

8. Years of professional work experience in related field :  
(check one).

- Less than 2 years
- 2 - 5 years
- 10 - 15 years
- 5 - 10 years
- More than 15 years

9. Highest Educational level attained : (check one)

- Bachelor's Degree
- Master's Degree
- Doctoral Degree
- Full Professional Degree

10. Subjects taken as Optional/Honours in Undergraduate Degree

---

---

11. Subjects taken as Compulsory/Minor in Undergraduate Degree

---

---

12. Subjects taken as Majors in Postgraduate Degree

---

---

13. Subjects taken in Professional Body Exam of  
ICAI/ICWAI/ICMA/ICSI etc.:

---

---

---

14. Significant Training Obtained in Systems auditing :

---

---

---

---

---

15. Memberships in Professional Bodies :

---

---

---

---

16. Professional Certifications obtained :

---

---

---

17. Indicate your level of Technical Expertise as follows :

HI - Knowledgeable and comfortable in dealing

MED - Familiar with major technical concepts

LO - Relatively unfamiliar with the technology

(check all that apply)

	HI	MED	LO
Application Systems Programming	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Computer Operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Computer Resource Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Database Administration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Communication Network Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Communication Network Operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information Systems Planning	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Methods & Procedures Analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Operating Systems Programming	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Systems Analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Systems Documentation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial Auditing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information Systems Auditing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial Accounting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Managerial Accounting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Processing Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (List below)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-----	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-----	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-----	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

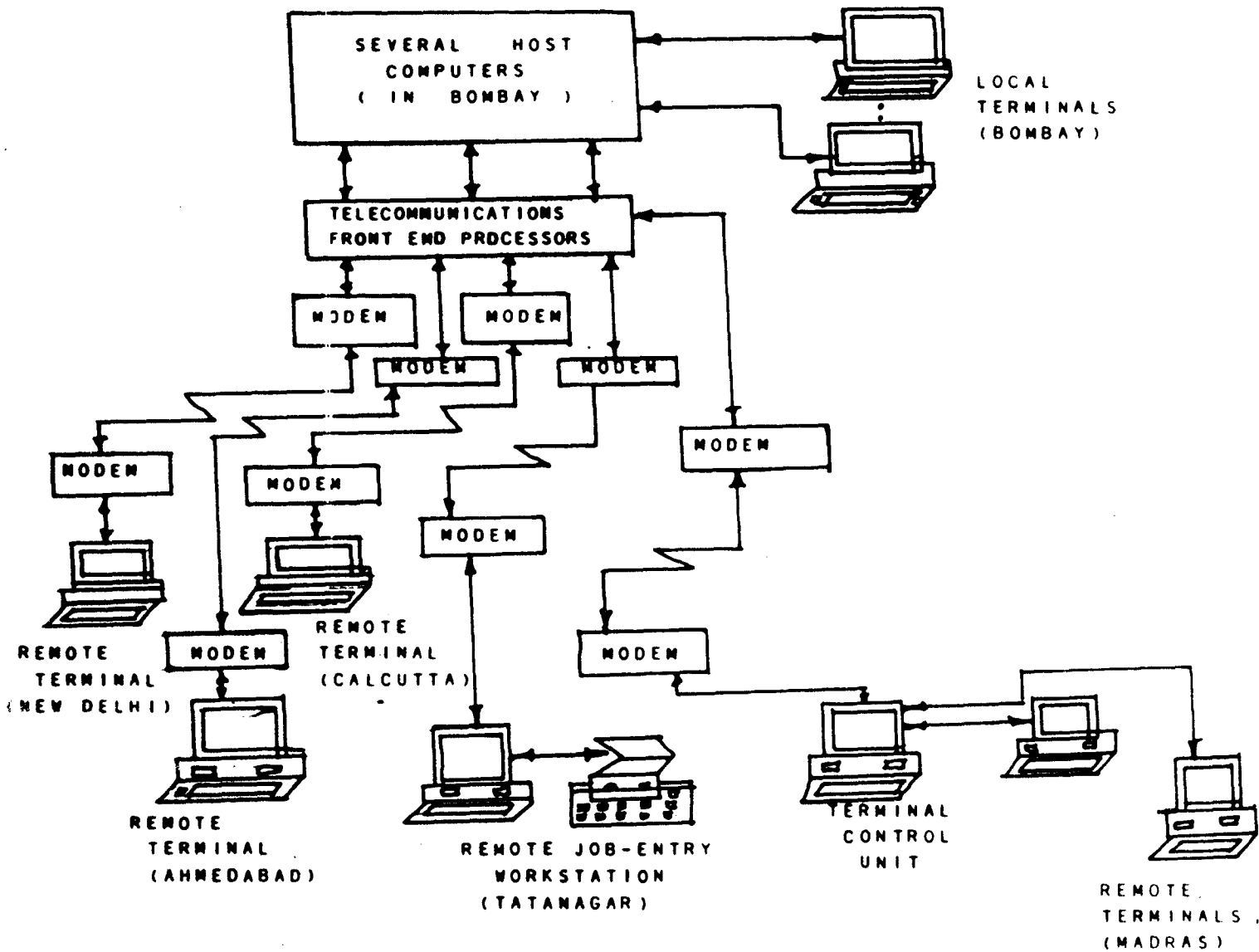


Figure 1 : Hypothetical example of A Traditional Systems Networking Environment



**Scenario A : Questionnaire**

Please consider the Scenario described above carefully and answer each of the following questions accordingly.

In order to EFFECTIVELY PLAN AN INFORMATION SYSTEMS AUDIT in a scenario A environment, I need :

1. To have advanced training in telecommunications networking Technologies.

Strongly Disagree	----- ----- ----- ----- -----  1          2          3          4          5	Strongly Agree
Non Critical For Success	----- ----- ----- ----- -----  1          2          3          4          5	Critical For Success

2. To utilise a participative management approach in dealing with the audit team members :

Strongly Disagree	----- ----- ----- ----- -----  1          2          3          4          5	Strongly Agree
Non Critical For Success	----- ----- ----- ----- -----  1          2          3          4          5	Critical For Success

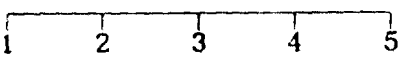
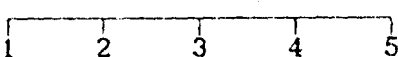
3. To utilise technical specialists in specific areas of telecommunication technology.

Strongly Disagree	----- ----- ----- ----- -----  1          2          3          4          5	Strongly Agree
Non Critical For Success	----- ----- ----- ----- -----  1          2          3          4          5	Critical For Success

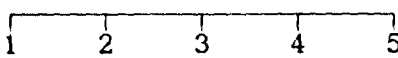
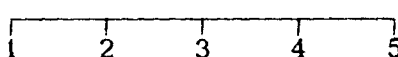
4. To have advanced training in Non - EDP auditing techniques and procedures.

Strongly Disagree	----- ----- ----- ----- -----  1          2          3          4          5	Strongly Agree
Non Critical For Success	----- ----- ----- ----- -----  1          2          3          4          5	Critical For Success

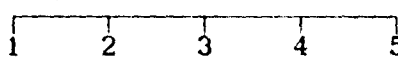
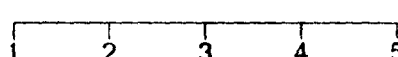
5. To have experience as a computer operator.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

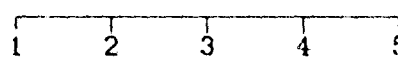
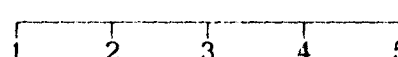
6. To review the completeness of the system audit plan based upon the individual situation to be audited.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

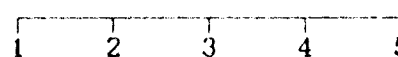
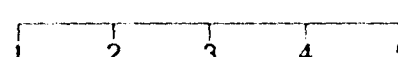
7. To have advanced training in computer systems topics such as computer operations, applications systems, and the management of technological change.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

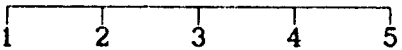
8. To review the relevance of each planned systems audit activity in terms of its contribution to achieving appropriate audit objectives.

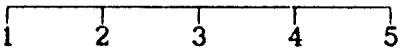
Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

9. To be trained in database management systems concepts.

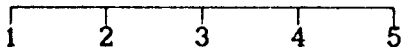
Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

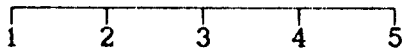
10. To have experience doing application systems development work.

Strongly Disagree  Strongly Agree

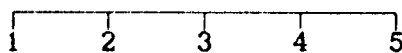
Non Critical For Success  Critical For Success

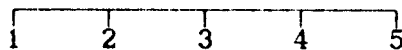
11. To establish the proper mix of personnel and skills to cover all categories of technical expertise to be utilised in the audit.

Strongly Disagree  Strongly Agree

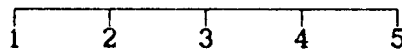
Non Critical For Success  Critical For Success

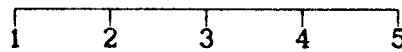
12. To have access to models for example data reduction, forecasting, or systems simulation.

Strongly Disagree  Strongly Agree

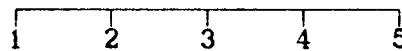
Non Critical For Success  Critical For Success

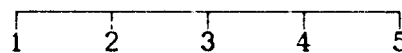
13. To be trained in time-sharing application techniques.

Strongly Disagree  Strongly Agree

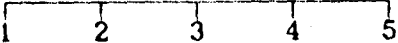
Non Critical For Success  Critical For Success

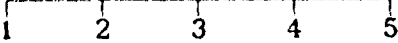
14. To have experience doing operating systems programming tasks

Strongly Disagree  Strongly Agree

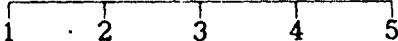
Non Critical For Success  Critical For Success

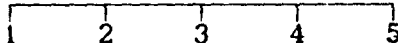
15. To have experience doing operating systems programming tasks.

Strongly Disagree  Strongly Agree

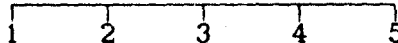
Non Critical For Success  Critical For Success

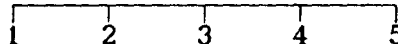
16. To have experience as a data base systems developer.

Strongly Disagree  Strongly Agree

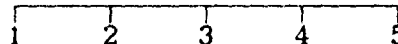
Non Critical For Success  Critical For Success

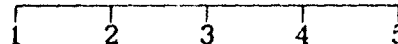
17. To be trained in applications systems concepts and techniques.

Strongly Disagree  Strongly Agree

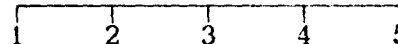
Non Critical For Success  Critical For Success

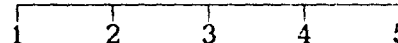
18. To be trained in non-EDP audit concepts and analytic techniques.

Strongly Disagree  Strongly Agree

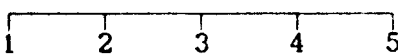
Non Critical For Success  Critical For Success

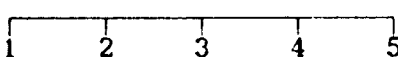
19. To be trained in tele-communications systems technology.

Strongly Disagree  Strongly Agree

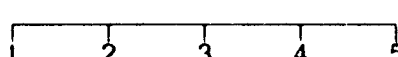
Non Critical For Success  Critical For Success

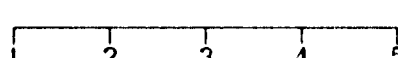
20. To have experience as a time-sharing systems on-line programmer.

Strongly Disagree  Strongly Agree

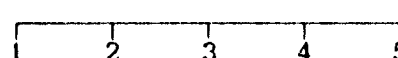
Non Critical For Success  Critical For Success

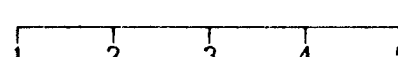
21. To utilise technical specialists in specific areas of computing systems technology.

Strongly Disagree  Strongly Agree

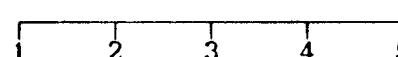
Non Critical For Success  Critical For Success

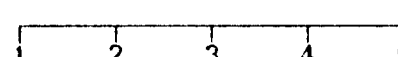
22. To maintain a long term perspective for the audit process even during short-term planning activities.

Strongly Disagree  Strongly Agree

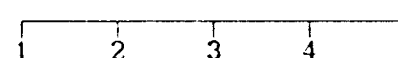
Non Critical For Success  Critical For Success

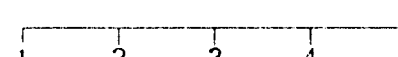
23. To be trained in computer operations concepts and techniques.

Strongly Disagree  Strongly Agree

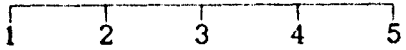
Non Critical For Success  Critical For Success

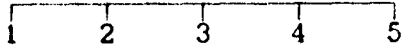
24. To be trained in distributed processing concepts and systems technology.

Strongly Disagree  Strongly Agree

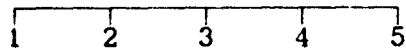
Non Critical For Success  Critical For Success

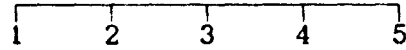
25. To have experience implementing distributed processing systems.

Strongly Disagree  Strongly Agree

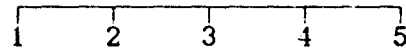
Non Critical For Success  Critical For Success

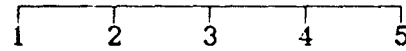
26. To be trained in information systems management concepts and methodologies.

Strongly Disagree  Strongly Agree

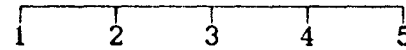
Non Critical For Success  Critical For Success

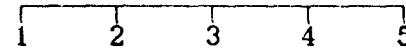
27. To document the systems audit plan for each audit prior to the beginning of the engagement.

Strongly Disagree  Strongly Agree

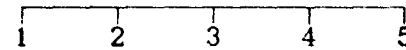
Non Critical For Success  Critical For Success

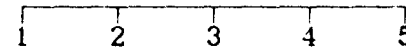
28. To have access to hardware or software monitors.

Strongly Disagree  Strongly Agree

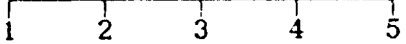
Non Critical For Success  Critical For Success

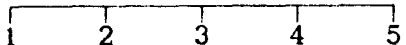
29. To review decisions regarding the systems audit with non systems audit personnel.

Strongly Disagree  Strongly Agree

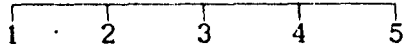
Non Critical For Success  Critical For Success

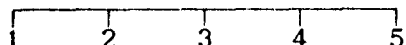
30. To define the objectives of the systems audit specifically for each individual situations.

Strongly Disagree  Strongly Agree

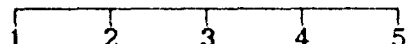
Non Critical For Success  Critical For Success

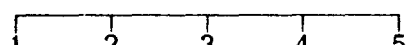
31. To be trained in operating systems concepts & techniques.

Strongly Disagree  Strongly Agree

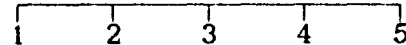
Non Critical For Success  Critical For Success

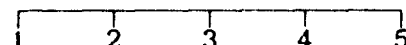
32. To have access to a range of technical library materials.

Strongly Disagree  Strongly Agree

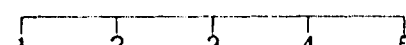
Non Critical For Success  Critical For Success

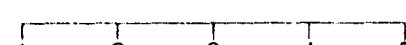
33. To have experience as a telecommunications analyst.

Strongly Disagree  Strongly Agree

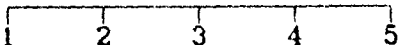
Non Critical For Success  Critical For Success

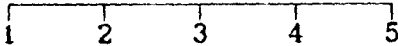
34. To utilise technical specialists in specific areas of information systems auditing.

Strongly Disagree  Strongly Agree

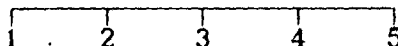
Non Critical For Success  Critical For Success

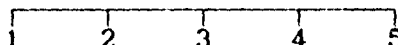
35. To have experience in managing information system.

Strongly Disagree  Strongly Agree

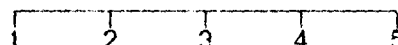
Non Critical For Success  Critical For Success

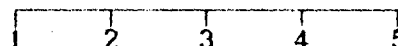
36. To have access to standardised audit methodologies, procedures, and techniques.

Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success

37. To have access to reporting software to evaluate systems usage levels.

Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success



## SCENARIO B

### COMPLEX COMPUTING AND NETWORKING ENVIRONMENT

Scenarios A and B are intended to relate to similar business environments. You should assume in answering the following questions that the only differences between the companies represented and their data processing environments deals with the degree to which each uses computer communication facilities. Scenario B is described as follows :

Consider a distributive systems environment in which computing is decentralised at several processing nodes. Some of these include large-scale mainframes and some include various sized mini and micro computers. This array of computing equipment is interconnected by a sophisticated network consisting of private leased lines, gateway connections into LAN facilities that tie directly into the private network, and (perhaps) an integrated telephone switching system. The network includes concentrator equipment at key nodes and supports a variety of network protocols depending upon the requirements associated with the computing equipment utilized at each nodes. Disk and tape storage facilities are located at nodes in the network wherever needed. Technical and user support functions are provided by staff including computer operation, operating systems programming, applications systems programming, customer services and administrative departments. Applications performed include mostly traditional batch and time sharing,

specialised software on intelligent workstations of various kinds, and numerous evolving office automation applications.

-----

Please give the estimated number of information systems audits in "Scenario B" environments in which you have participated during :

1991 \_\_\_\_\_ 1980 - 85 \_\_\_\_\_

1990 \_\_\_\_\_ 1985 - 90 \_\_\_\_\_

(Answer all that are appropriate)

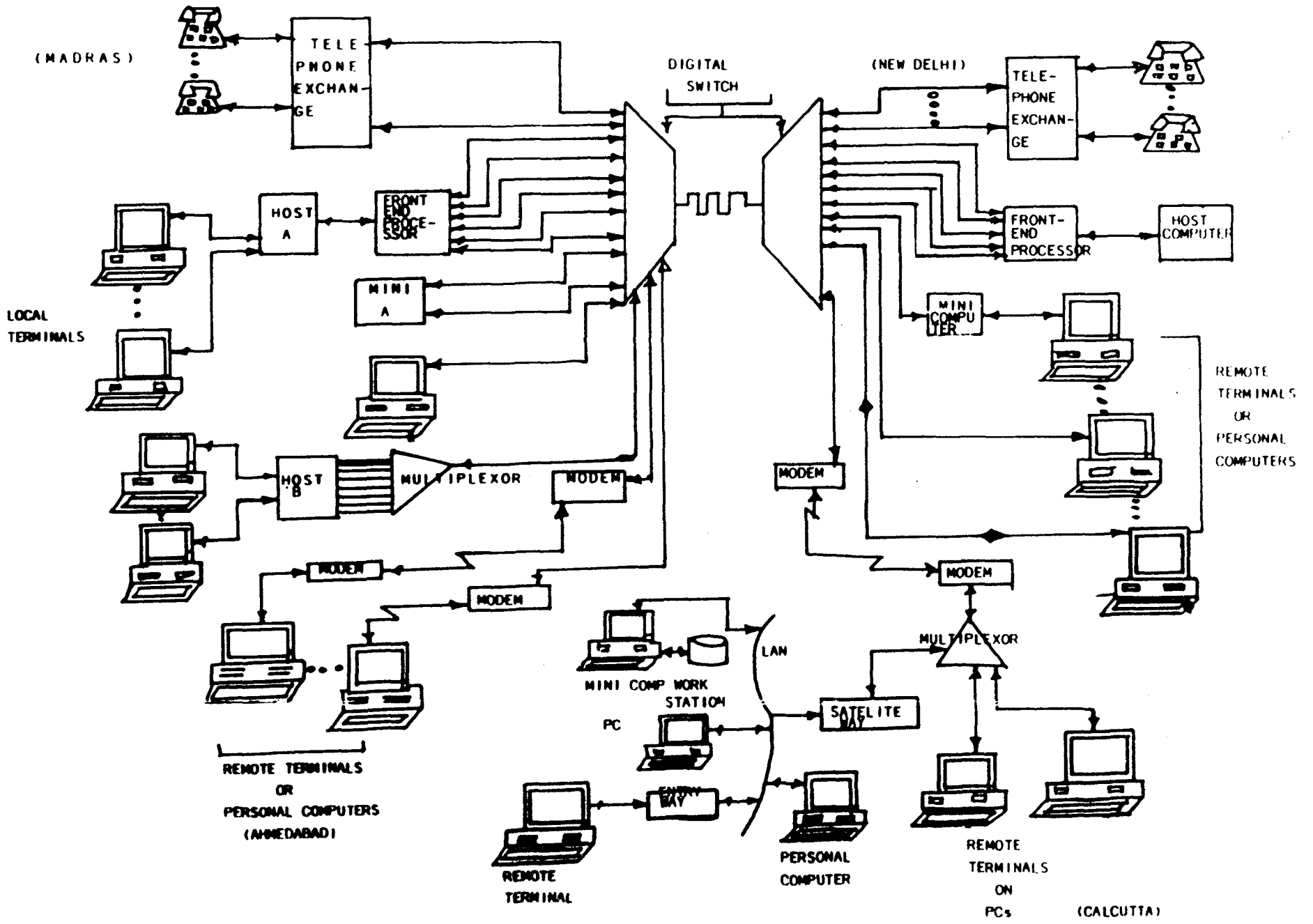


Figure 2 : Hypothetical example of a Complex Systems Networking Environment

**Scenario B : Questionnaire**

Please consider the Scenario described above carefully and answer each of the following questions accordingly :

In order to EFFECTIVELY PLAN AN INFORMATION SYSTEMS AUDIT in a Scenario B environment, I need :

1. To review the completeness of the system audit plan based upon the individual situation to be audited.

Strongly Disagree	1 ————— 2 ————— 3 ————— 4 ————— 5	Strongly Agree
Non Critical For Success	1 ————— 2 ————— 3 ————— 4 ————— 5	Critical For Success

2. To have experience in managing information system environments.

Strongly Disagree	1 ————— 2 ————— 3 ————— 4 ————— 5	Strongly Agree
Non Critical For Success	1 ————— 2 ————— 3 ————— 4 ————— 5	Critical For Success

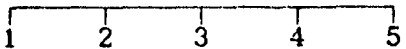
3. To be trained in tele-communications systems technology.

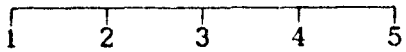
Strongly Disagree	1 ————— 2 ————— 3 ————— 4 ————— 5	Strongly Agree
Non Critical For Success	1 ————— 2 ————— 3 ————— 4 ————— 5	Critical For Success

4. To have access to a range of technical reference library materials.

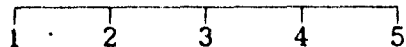
Strongly Disagree	1 ————— 2 ————— 3 ————— 4 ————— 5	Strongly Agree
Non Critical For Success	1 ————— 2 ————— 3 ————— 4 ————— 5	Critical For Success

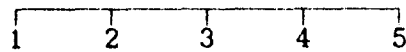
5. To have experience doing Non-EDP auditing.

Strongly Disagree  Strongly Agree

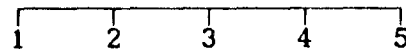
Non Critical For Success  Critical For Success

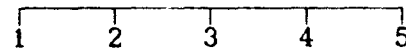
6. To have access to standardised audit methodologies, procedures, and techniques.

Strongly Disagree  Strongly Agree

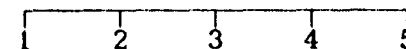
Non Critical For Success  Critical For Success

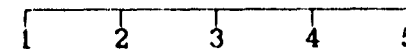
7. To have experience as a data base systems developer.

Strongly Disagree  Strongly Agree

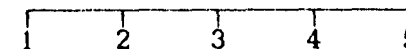
Non Critical For Success  Critical For Success

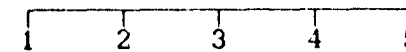
8. To have advanced training in computer systems topics such as computer operations, applications systems, and the management of technological change.

Strongly Disagree  Strongly Agree

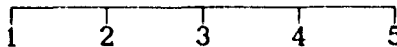
Non Critical For Success  Critical For Success

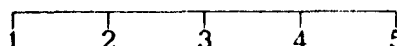
9. To have access to hardware or software monitors.

Strongly Disagree  Strongly Agree

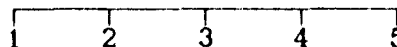
Non Critical For Success  Critical For Success

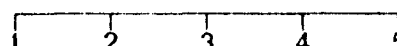
10. To utilise technical specialists in specific areas of telecommunications technology.

Strongly Disagree  Strongly Agree

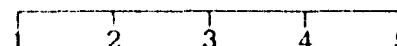
Non Critical For Success  Critical For Success

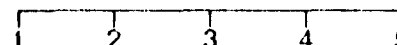
11. To be trained in operating systems concepts & techniques.

Strongly Disagree  Strongly Agree

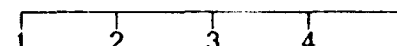
Non Critical For Success  Critical For Success

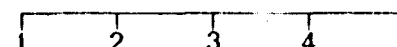
12. To have advanced training in Non - EDP auditing techniques and procedures.

Strongly Disagree  Strongly Agree

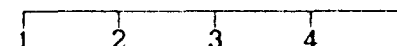
Non Critical For Success  Critical For Success

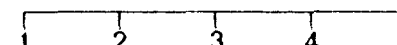
13. To utilise technical specialists in specific areas of information systems auditing.

Strongly Disagree  Strongly Agree

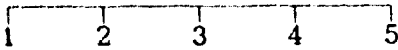
Non Critical For Success  Critical For Success

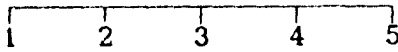
14. To be trained in information systems management concepts and methodologies.

Strongly Disagree  Strongly Agree

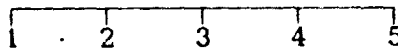
Non Critical For Success  Critical For Success

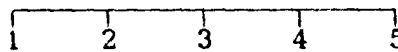
15. To have advanced training in telecommunications networking Technologies.

Strongly Disagree  Strongly Agree

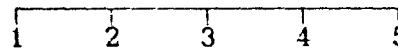
Non Critical For Success  Critical For Success

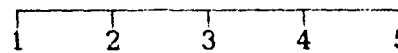
16. To have experience as a telecommunications analyst.

Strongly Disagree  Strongly Agree

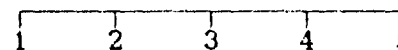
Non Critical For Success  Critical For Success

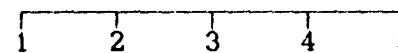
17. To have access to models, for example data reduction, forecasting, or systems simulation.

Strongly Disagree  Strongly Agree

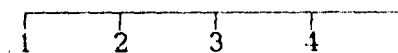
Non Critical For Success  Critical For Success

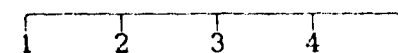
18. To document the systems audit plan for each audit prior to the beginning of the engagement.

Strongly Disagree  Strongly Agree

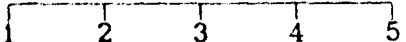
Non Critical For Success  Critical For Success

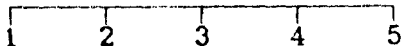
19. To be trained in applications systems concepts and techniques.

Strongly Disagree  Strongly Agree

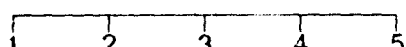
Non Critical For Success  Critical For Success

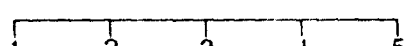
20. To utilise a participative management approach in dealing with the audit team members :

Strongly Disagree  Strongly Agree

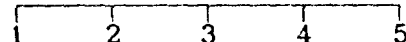
Non Critical For Success  Critical For Success

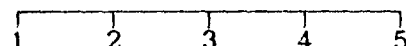
21. To define the objectives of the systems audit specifically for each individual situations.

Strongly Disagree  Strongly Agree

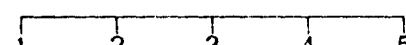
Non Critical For Success  Critical For Success

22. To be trained in time-sharing application techniques.

Strongly Disagree  Strongly Agree

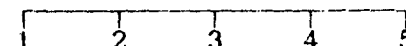
Non Critical For Success  Critical For Success

23. To utilise technical specialists in specific areas of computing systems technology.

Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success

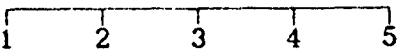
24. To have experience as a computer operator.

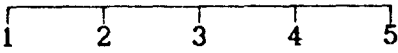
Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success

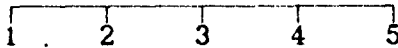


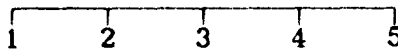
25. To be trained in database management systems concepts.

Strongly Disagree  Strongly Agree

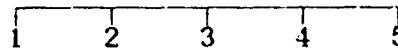
Non Critical For Success  Critical For Success

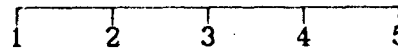
26. To review decisions regarding the systems audit with non-systems audit personnel.

Strongly Disagree  Strongly Agree

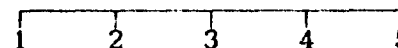
Non Critical For Success  Critical For Success

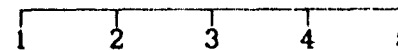
27. To be trained in distributed processing concepts and systems technology.

Strongly Disagree  Strongly Agree

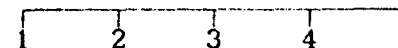
Non Critical For Success  Critical For Success

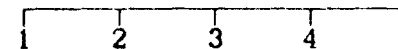
28. To have experience implementing distributed processing systems.

Strongly Disagree  Strongly Agree

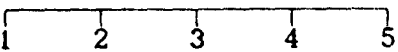
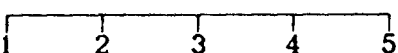
Non Critical For Success  Critical For Success

29. To be trained in Non-EDP audit concepts and analytic techniques.

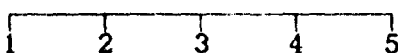

Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success

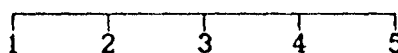
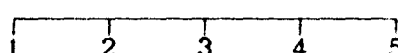
30. To review the relevance of each planned systems audit activity in terms of its contribution to achieving appropriate audit objectives.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

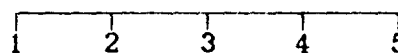
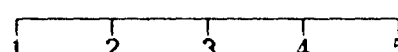
31. To have experience doing application systems development work.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

32. To maintain a long-term perspective for the audit process even during short-term planning activities.

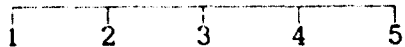
Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

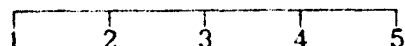
33. To establish the proper mix of personnel and skills to cover all categories of technical expertise to be utilized in the audit.

Strongly Disagree  Strongly Agree  
Non Critical For Success  Critical For Success

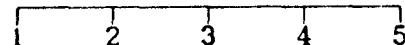


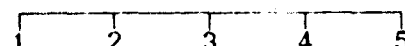
34. To be trained in computer operation concepts and techniques.

Strongly Disagree  Strongly Agree

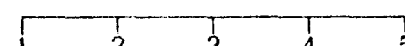
Non Critical For Success  Critical For Success

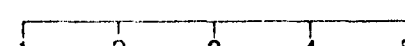
35. To have experience as a time-sharing systems on-line programmer.

Strongly Disagree  Strongly Agree

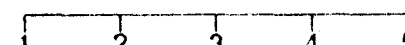
Non Critical For Success  Critical For Success

36. To have experience as a time-sharing systems on-line programmer.

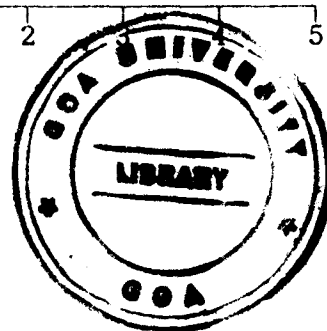
Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success

37. To have access to reporting software to evaluate systems usage levels.

Strongly Disagree  Strongly Agree

Non Critical For Success  Critical For Success



THANK YOU FOR YOUR CO-OPERATION