



UNIVERSITY
OF
JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION



- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.
- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

Surname, Initial(s). (2012) Title of the thesis or dissertation. PhD. (Chemistry)/ M.Sc. (Physics)/ M.A. (Philosophy)/M.Com. (Finance) etc. [Unpublished]: [University of Johannesburg](https://ujdigispace.uj.ac.za). Retrieved from: <https://ujdigispace.uj.ac.za> (Accessed: Date).

ET) 10
BOSH

THE INTERFACE BETWEEN APPLICATION CONTROLS
AND INTEGRITY CONTROLS IN MODERN COMPUTER SYSTEMS

by

WILLEM HENDRIK BOSHOFF

DISSERTATION

submitted in fulfillment of the requirements for the degree

MASTER IN ECONOMIC SCIENCES

in

ACCOUNTING AND AUDITING

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RANDSE AFRIKAANSE UNIVERSITEIT

STUDY LEADER: PROF. F.J. NEL

MAY 1985

INDEX

	<u>Page No.</u>
INTRODUCTION	1 - 11
LITERATURE SURVEY	12 - 34
COMPUTER CONTROL HYPOTHESIS - CONCEPTS AND DEFINITIONS	35 - 43
COMPUTER CONTROL HYPOTHESIS - INTERFACING APPLICATION AND INTEGRITY CONTROLS	44 - 59
VALIDITY OF THE CONTROL MODEL AND THE INTERFACE HYPOTHESIS	60 - 87
BIBLIOGRAPHY	88

**DIE KOPPELVLAK TUSSEN TOEPASSINGS-EN INTEGRITEITSKONTROLES IN MODERNE
REKENAARSTELSLS**

DEUR

WILLEM HENDRIK BOSHOFF

**OPSOMMING VAN VERHANDELING INGEDIEN
VIR DIE GRAAD MAGISTER IN REKENINGKUNDE-EN
ODITKUNDE IN DIE FAKULTEIT EKONOMIESE-EN
BESTUURSWETENSKAPPE BY DIE RANDSE AFRIKAANSE UNIVERSITEIT**

STUDIELEIER: PROF. F.J. NEL

MEI 1985

Die doel van die opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing oor rekenaarbeheer weer te gee. Hierdie opsomming is onder die volgende hoofde uiteengesit:

I. PROBLEEMOMSKRYWING EN DOEL VAN HIERDIE NAVORSING

II. NAVORSINGSONTWERP EN METODIEK

III. GEVOLGTREKKINGS

I. PROBLEEMOMSKRYWING EN DOEL VAN HIERDIE NAVORSING

Eksterne en interne ouditeure is betrokke by rekenaarstelsels wat al hoe meer ingewikkeld word. Die ouditeur se belang in so 'n omgewing is primer 'n studie van die beheermaatreëls oor die rekenaarstelsel en die risiko van foute en bedrog. As gevolg van die ingewikkeldheid van rekenaar-tegnologie het navorsing oor beheermaatreëls nie tred gehou met moderne tegnologie nie en gevolglik is baie kritiek na die ouditeur gerig vanweë hulle onvermoë om by te hou.

Hierdie navorsing is gedoen om 'n konseptuele grondslag daar te stel wat die basis kan vorm vir die ontwikkeling van metodieke om gevorderde stelsels mee te oudit. Een van die grootste struikelblokke in hierdie verband is om die spesifieke rol van die rekenaar en die onderliggende programmatuur te verstaan. Hierdie verhandeling is spesifiek om hierdie rol te ondersoek en te bepaal hoe die gebruiker-en dataverwerkingkomponente in 'n stelsel koppel.

Ten einde die studieveld af te baken en sodoende betekenisvolle studie te kon doen is 'n aantal beperkinge gespesifiseer wat ons volg opgesaam word.

- (i) Die doel van hierdie navorsing is beperk tot spesifieke teoretiese konsepte van rekenaarbeheer en geen poging is aangewend om beheertegniese te ondersoek of hoe die konsepte in 'n ouditmetodiek geïmplementeer kan word nie.
- (ii) Die navorsing is gerig op 'n konseptuele vlak en besonderhede oor beheertegniese en die relatiewe voordele van elk was buite hierdie studieveld gereken.
- (iii) As gevolg van die omvang van rekenaarsekerheid, verdeling van pligte en magtiging van transaksies en die aard van hulle onderlinge koppeling is hierdie onderwerp slegs op oorsigtelike basis gedek. Hierdie veld word beskou as 'n aparte studierigting en 'n poging om meer besonderhede oor hierdie onderwerp te verskaf sou afbreek gedoen het aan die hoofdoel van hierdie verhandeling.

II. NAVORSINGSONTWERP EN METODIEK

Ten einde 'n koppeling tussen rekenaartegnologie en besigheidsprosedures te verseker is die navorsing gerig op drie afsonderlike aspekte.

(i) Rekenaartegnologie

(ii) Huidige EDV Ouditpraktyk

(iii) Rol van die rekenaar in 'n stelsel

Hierdie benadering is nodig geag om elke aspek te vereenvoudig en sodoende 'n volledige en logiese ondersoek te verseker. 'n Navorsingsontwerp is vir elke onderwerp afsonderlike opgestel. Huidige EDV Ouditpraktyk is ondersoek met behulp van 'n literatuuroorsig; rekenaartegnologie met verwysing na spesifieke literatuur en die rol van die rekenaar is ondersoek deur van 'n hipotese gebruik te maak.

Spesifieke aandag is geskenk om die geldigheid en gesaghebbendheid van die literatuur wat gebruik is te bewys ten einde 'n aanvaarbare grondslag te verseker.

III. GEVOLGTREKKINGS

Die fundamentele doelstellings van beheermaatreëls verskil geensins in 'n rekenaarstelsel nie. Hierdie doelstellings kan soos volg geklassifiseer word.

- | | |
|---|--|
| (i) Volledigheid van invoer en verwerking. | alle data word ingevoer en verwerk. |
| (ii) Akkuraatheid van invoer en verwerking. | data word korrek verwerk. |
| (iii) Geldigheid van invoer. | slegs geldige of gemagtigde data word verwerk. |
| (iv) Onderhoud. | data word nie verander na verwerking nie. |

Die verskil tussen 'n hand- en 'n rekenaarstelsel is die beheertegniese beskikbaar en die spesiale oorwegings in rekenaarstelsels as gevolg van laasgenoemde se gebrek aan intelligensie. Beheertegniese kan geklassifiseer word as:

- (i) Toepassingskontroles; kontroles wat deur gebruikers uitgevoer word.
- (ii) Integriteitskontroles; kontroles wat deur die dataverwerkingafdeling uitgevoer word.

Beheertegnieke kan op die rekenaar steun. Dit is egter noodsaaklik dat een komponent, opvolging van foute en uitsonderings, deur 'n persoon gedoen word. Hierdie beperking is as gevolg van die onvermoë van 'n rekenaar om nie-roetine funksies uit te voer. Integriteitskontroles wat op die rekenaar steun kan of in toepassingsprogrammatuur of in stelselprogrammatuur ingebou word en word bepaal deur die omvang van die rekenarisering. Uit bogenoemde begrippe is dit moontlik om 'n verwantskap tussen die tipes beheermaatreëls te definieer. Hierdie verwantskap tussen toepassings- en integriteitskontroles is optimaal indien hulle op 'n gelyke vlak gedefinieer word aangesien dit optimale koppelvlakke moontlik maak. Die sterkste verwantskap is wanneer substitusie moontlik is terwyl aanvulling die ondergeskikte is. Eersgenoemde is moontlik wanneer taakintegriteit en die voorkoming van foute en ongemagtigde verwerking betrokke is terwyl laasgenoemde nodig is wanneer 'n toepassing direk beheer word.

Hierdie navorsing is waardevol vir ouditeure aangesien dit moontlik is om:

- (a) Verdere insig in die beheer van moderne rekenaarstelsels te verkry.
- (b) Oudittegnieke te ontwikkel binne die teoretiese raamwerk wat daargestel is.
- (c) Die rol wat rekenaar-tegnologie op beheer speel in terme van die konseptuele grondslae te verstaan.

Aangesien oudit nog 'n dissipline is kan hierdie navorsing navorsers help om dit 'n stap nader aan 'n wetenskap te bring.

INTRODUCTION

The objective of this section is to provide the background methodologies and conclusions of this research in the area of computer controls. This section is presented under the following headings:

- I PROBLEM DESCRIPTION AND OBJECTIVE OF THIS RESEARCH
- II RESEARCH APPROACH
- III RESEARCH METHODOLOGY
- IV CONSTRAINTS AND EXCLUSIONS
- V CONCLUSION

I PROBLEM DESCRIPTION AND OBJECTIVE OF THIS RESEARCH

External and Internal auditors have to deal with computer systems which are becoming increasingly complex. An auditor's interest in such an environment is primarily an understanding of the controls over the computer system and the risk of error and fraud. When dealing with controls two issues are important. The first deals with the ability to control a complex computer system. Unless the control issues are understood and the impact of various alternatives appreciated it would be impossible to control a computer system. Under such circumstances there is a high risk of error and fraud and the information present in a business could be very unreliable.

Secondly the auditor needs to evaluate controls for purposes of his audit. Usually the objective is to assure himself that they adequately safeguard the business assets and prevent or detect errors present in the accounting records of the concern.

It may however also be necessary to consider such issues as fraud or misappropriation of assets and efficiency of internal controls.

In a modern computer system one finds integrated application systems eg. debtors and stock integrated with a general ledger with many of the routine procedures which were previously performed by users now automated. Examples of modern computer systems are on-line, real time and data base applications where transactions are initiated and processed at the point where they originate. Often little or no hardcopy evidence is present and traditional audit trails for tracing the final transaction back to underlying source documents may be impossible. The advent of computers has also led to data reduction requirements, eg. summary reports. In most instances such summaries cannot be rechecked as the underlying data will have changed since the summary was produced.

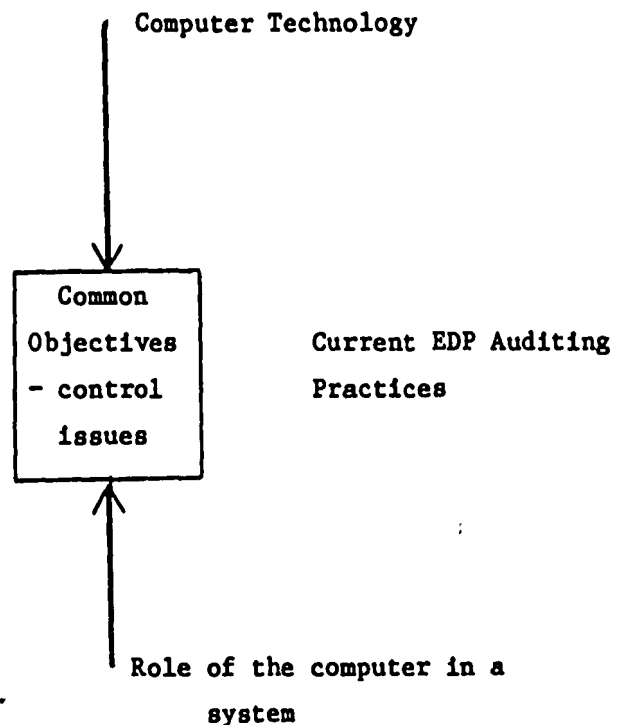
Auditors have realised that they have to respond to changes in technology. The complexity and pervasiveness of current technology has however caused research in the area of computer controls to lag behind current computer technology and harsh criticism has been directed at auditors for failing to keep up with such technology.

The research undertaken to prepare this paper has been done in order to investigate and develop the conceptual foundations which could form the basis for developing auditing methodologies in sophisticated computer systems. One of the biggest stumbling blocks in controlling modern computer systems in practice is to understand the role of the computer and its software in specific application environments. In other words, how does the user component of a system and the data processing component link and to what extent does this link impact on controls? This dissertation termed "interfacing application controls (or user controls) and integrity controls (or controls over data processing)" is the result of the investigation of the impact of the link between the two types of controls. The results of research of this nature may be valuable to auditors and computer control experts for a number of reasons:

- (i) It will enable them to gain further insight into control issues in modern computer systems.
- (ii) A theoretical base for developing auditing tools and techniques which can be used to overcome present shortcomings in this area is made available.
- (iii) It provides the conceptual foundation for understanding the impact of modern technology on controls and the role of the computer system and its underlying software.
- (iv) As auditing is still a discipline this research will assist further researchers in advancing it towards becoming a science.

II RESEARCH APPROACH

Two things are apparent from the current criticism of auditors in the data processing environment. The first is their lack of data processing knowledge and the second is their tendency to classify the user component of a system and the data processing component as unrelated issues. To address these issues this research has been approached on the basis that cognisance should be taken of computer technology and its role or link with business procedures. To achieve this, research has been directed at three separate areas with common objectives. The following diagram illustrates the approach taken:



There are a number of reasons for approaching the research in this manner:

- (i) It is simpler to investigate the specific objectives in each separate area rather than attempt to cover all areas simultaneously.
- (ii) Presentation of one topic at a time is more convenient and logical.
- (iii) It ensures comprehensive coverage in each area.

The nature of this research approach does, however, create the need for a research methodology in each area.

III RESEARCH METHODOLOGY

A. CURRENT EDP AUDIT PRACTICES

Establishing the nature and extent of current EDP auditing practices requires a review of available and appropriate authoritative sources of reference on the topic. To achieve an adequate coverage without spending a disproportionate amount of time and effort in any one area, a literature survey of publications published or endorsed by various professional bodies was carried out. The bodies selected were:

The American Institute of Certified Public Accountants

The Canadian Institute of Chartered Accountants

The Institute of Chartered Accountants in England and Wales

The Institute of Internal Auditors

The major reason for selecting the above bodies is the number of auditors they represent. It is a reasonable assumption that the contents of the selected publications were well researched and contain authoritative views.

The objective of the literature survey was not only to highlight current audit practices but to provide a basis for developing the research contained in this dissertation.

Two other possible ways of establishing current EDP audit practice would be to:

- (i) conduct a survey of approaches adopted by various accounting firms and internal audit departments or,
- (ii) carry out an extensive literature study.

SURVEY OF ACCOUNTING FIRMS AND INTERNAL AUDIT DEPARTMENTS

To achieve the degree of authority the selected publications provide, it would have been necessary to survey a large number of firms and companies with internal audit departments. This would have resulted in a complete research project and it is reasonable to assume that respondents would have referred to professional publications for auditing methodologies used. Achieving international coverage would have been impracticable whereas the selected research methodology achieves this.

CARRYING OUT AN EXTENSIVE LITERATURE STUDY

Numerous problems with this approach are evident. For example it would have been extremely difficult to differentiate between authoritative and non-authoritative sources objectively. It would also be difficult to assess to what extent the study represented the audit and internal audit profession. After consideration of these factors it was concluded that maximum coverage of current EDP audit practices could be obtained by adopting the approach selected.

The other part of the research approach is the common objectives mentioned previously. For purposes of this dissertation these relate to a model for auditing computer systems and the interface between application and integrity controls. The scope of literature survey was therefore limited to achieve the specified objectives. This was considered necessary to ensure that the survey concentrated on relevant issues.

B. COMPUTER TECHNOLOGY

The criteria for developing a methodology for the computer technology component of this dissertation presented unique problems. A detailed analysis of modern technology or a survey of specific manufacturers falls outside the scope of this dissertation. Analysis of the literature requirements provided the following specifications:

- (i) The publications had to be current, authoritative and based on comprehensive research studies.
- (ii) Treatment of the whole range of system software present in a modern computer needed to be covered at an overview level.
- (iii) Practical issues needed to be covered rather than mathematical treatment of individual system software subjects.

The same approach described under current EDP audit practices has been adopted here. A publication sponsored and authored by a representative of International Business Machines was considered representative of a major part of current technology. A very recent publication was selected as, in addition to being based on sound research it contained the functional components of modern technology, which is the primary issue in this dissertation.

Again there are arguments against adopting this type of methodology but the relative advantages outweigh the disadvantages for the reasons presented in the above paragraphs.

C. ROLE OF THE COMPUTER IN A SYSTEM

Whilst the inconclusiveness of literature survey of current EDP audit practices confirmed the need for research of this nature a number of important control issues in modern computer systems were highlighted. With inadequate literature support the only alternative approach to this research was by way of hypothesis. The methodology used to achieve this can be summarised as follows:

- (i) The definitions and postulates used in the dissertation were established.
- (ii) A general hypothetical model for evaluating computer controls and specifying an interface between application and integrity controls was established.

- (iii) Based on the general model a detailed hypothesis for the interface between application and integrity controls was developed.
- (iv) Using aspects from the current EDP audit practices section the computer technology section and via a process of deductive analysis the general and detailed hypothesis were confirmed.
- (v) To contain the extent of this dissertation a number of constraints and exclusions were necessary. These, together with the conclusions arrived at are set out below.

IV CONSTRAINTS AND EXCLUSIONS

Computer controls is such a vast topic that some constraints and exclusions are essential. The constraints are summarised as follows:

- (i) The objective of the research is limited to specific theoretical concepts of computer controls and no attempt has been made to review detailed control techniques or how such concepts could be implemented in an audit methodology.
- (ii) Research has been directed at the conceptual level and details of specific control techniques such as batching, edit checks, and the relative merits of each is considered outside the scope of this dissertation.

Due to its complexity the area of computer security, division of duties and authorisation of transactions which interact extensively in a modern computer system was dealt with briefly and in overview fashion only. The reason for excluding a detailed review is that to appreciate the impact of computer security, division of duties and authorisation, an understanding of error, fraud and information confinement needs to be obtained. Whilst it may appear that a simple solution is apparent the following example illustrates some of the complex issues.

- (i) What constitutes division of duties in an on-line system where the user carries out end-user programming or runs programs himself?
- (ii) Assuming that effective controls always include some manual procedures to what extent can division of duties be automated? Does computer security achieve this?
- (iii) Are there differences between the nature of controls required to safeguard against unintentional error, intentional error or fraud? How does this impact on application controls and integrity controls? What role does computer security play in this?

In the researcher's opinion this subject is a complete field of study on its own and any attempt to deal with these issues in any amount of detail would have detracted from the objective of this research project. Consequently this area is only dealt with insofar as it affected the objectives of this dissertation.

V CONCLUSION

The fundamental control and audit objectives which are present in manual systems do not change when the system is automated. These control objectives in broad terms are:

- | | |
|--|---|
| (i) Completeness of input and processing | all data is input and processed |
| (ii) Accuracy of input and processing | data is correctly processed |
| (iii) Validity of input | only valid or authorised data is processed. |
| (iv) Maintenance | data is not altered after processing. |

Essentially the differences between a manual and a computer system are the control techniques which are available to control the system and the special considerations that apply to a computer because of its lack of intelligence. The control techniques can be classified under two control types.

- (i) Application controls which are controls exercised by the users of the system and,
- (ii) Integrity controls which are controls exercised by the data processing departments.

Control techniques may be manual or computer based. It is however always essential that one component, following up of errors and exceptions, be manual. This is a constraint imposed by the inability of computer systems to perform non-routine procedures. Computer based controls exercised by the data processing department assumes two forms. They can either be incorporated in the application software or into system software. The extent of the automation of controls is dictated by the capabilities and restrictions of the computer. Because application and integrity controls have the same control objectives and the more complex systems require greater reliance on integrity controls the two control types can be considered at peer levels. The reason for the increased reliance on integrity controls in modern systems is the inefficiency and impracticability which often arises from trying to impose manual controls over systems where transactions are processed on-line from more than one terminal simultaneously. By regarding application and integrity controls at peer levels it is possible to determine how control techniques associated with one control type can be substituted by one from the other type. It has been determined however, that a relationship of direct substitution between the control types is not always possible. The circumstances where substitution is not possible arise when an element of a transaction is controlled by a user using a computer based procedure. The computer can at best perform the routine procedures on which the control is based and ensure that the programs which execute those procedures have been appropriately implemented.

By defining the relationship between application and integrity controls as being either substitution or compensation the basis for interfacing application and integrity controls was established. This relationship is however, at the control technique level; the control objectives never change. In fact it can be said that application and integrity controls are simply useful classifications of control techniques. On this basis it is possible to define a sophisticated interface between application and integrity controls.

The specification of the interface highlights a few additional facts about controls in a computer environment. In essence there are two types of control techniques. Type 1 are those which are used directly for application control purposes. Type 2 are those which prevent or detect errors and unauthorised activities during processing. The latter therefore enforce the integrity of the various tasks being performed. It has been established that integrity controls cannot be used as type 1 controls directly. At best the substitution rules mentioned above apply. Integrity controls are however much better as type 2 controls as the computer can normally be used to provide the basis for control more consistently and reliably than people. The ideal relationship, substitution, applies when integrity controls can be used as an alternative to application controls. In applying these concepts the key factor is to determine under each control objective the requirements for type 1 or 2 control techniques. Having done this it is possible to assess the adequacy of controls by determining whether the required balance of application and integrity controls are in place.

In summary this research has provided a basis for understanding the nature of controls in a modern computer environment. It has established relationships between the user and data processing component of computer based systems. Some specific areas which would require future research have been highlighted. Although this dissertation does not include suggestions for implementing the approach it does provide a theoretical foundation for encouraging future research in the area of computer controls and computer auditing.

LITERATURE SURVEY

The literature survey is set out under the following headings:

- I OBJECTIVES, NATURE, SCOPE AND DEFINITIONS
- II FUNDAMENTAL ASPECTS OF THE REFERENCES
- III ANALYSIS OF REFERENCES
- IV BIBLIOGRAPHY

I OBJECTIVES, NATURE, SCOPE AND DEFINITIONS

A OBJECTIVES

In order to derive maximum benefit from the literature survey the objectives were defined to allow comparative analysis of references and to facilitate subsequent synthesis or formalisation of computer control theory. The objectives are:

- (a) To obtain authoritative views on computer controls which will form the basis for the synthesis of a more rigorous theory for interfacing application and integrity controls. Application controls are at this stage informally defined as user controls and integrity controls as controls over the data processing component of a system.
- (b) To define models for authoritative views used in the literature survey. The reasons for defining models are:-
 - (1) to ensure ease of comparative analysis of references; and

- (ii) to emphasise the linkage or interface between application and integrity controls.
- (c) To obtain specific comments on techniques or recommendations for dealing with computer controls on a total system basis. The total system includes both the user and data processing component of a computer system.

B NATURE OF THE LITERATURE STUDY

To ensure credibility and acceptance of the findings and proposals of this dissertation it is essential that the underlying concepts are based on authoritative views and are generally accepted among computer auditing professionals. Theory based on an individual's experience without taking generally accepted professional views into account may be subject to personal bias and specific environments. Other factors which may introduce bias are the background and absence of formal research. To avoid these potential problems the references were restricted to those published or endorsed by various professional bodies. The organisations found to be most active in the field of computer controls and which have been involved in publications of an acceptable standard are:

The American Institute of Certified Public Accountants (The AICPA)

The Canadian Institute of Chartered Accountants (The CICA)

The Institute of Chartered Accountants in England and Wales

The Institute of Internal Auditors (The IIA).

The reasons for choosing these bodies are:

- (a) Their views can be considered authoritative and generally accepted due to the number of professional people they represent.

- (b) They are all internationally recognised.
- (c) Their views form guidelines which are often followed by professionals to form the basis for their computer control approaches. In other cases members of the bodies are obliged to follow standards which often result from these references.
- (d) At the time of the literature survey no other references by similar bodies could be found.

It may be said that restricting the scope of the literature survey to four major professional bodies could inhibit constructive thought but the benefits of having sound basic concepts outweigh this possibility. Most articles in magazines were found to be technique orientated and informed auditors how to deal with specific environments. Comprehensive articles providing complete theory could not be traced. This is however, not intended as criticism. On the contrary, the magazines provide professional computer auditors with tools and techniques to cope effectively in the practical world.

C SCOPE OF THE LITERATURE STUDY

Because of the emphasis of this dissertation on the interface between application and integrity controls, it is necessary to limit the scope of the literature survey. It would for example be impractical to include various techniques, or to examine specific mechanisms in on-line and data base systems. To achieve the objectives of the literature survey it was necessary to examine and analyse the generic computer control concepts and issues. Generic implies that the theory should be true in any environment. Consequently the following restrictions were placed on the scope of the literature survey.

- (a) Only issues which dealt with computer controls were included. Sections in the references which dealt with non-related issues were thus excluded.
- (b) Checklists, control questionnaires and lists of techniques are by definition not always generic as they deal with specific applications or environments.

- (c) As the dissertation principally deals with application and integrity controls, references to other types of internal control have not been included. Care was taken that terminology differences did not result in reclassification and possible exclusion from the literature survey. The detailed analysis of the various references cover all the components.

A great deal of preparatory work was done to ensure that the dissertation was based on sound theory and the restrictions imposed did not detract from the overall objectives; in fact they enforced concentration on those issues which are relevant to a dissertation of this nature.

D UNDERLYING DEFINITIONS

The basic definitions used for application and integrity controls for purposes of the literature survey are not of any significance other than to provide comparative terminology. As a result more formal definitions have been omitted until later.

The definitions are:

Application Controls: Controls exercised by users over the preparation, input, processing and output of data. Although data may be transformed during processing the transformation can be regarded as a derivative of the original data. As a result terms such as information, reports, etc are not deemed to be a necessary element of the definition.

Integrity Controls : Controls exercised by the data processing department to ensure that the programmed procedures relied on by the users to exercise controls have been properly implemented and operate effectively at all times. The term programmed procedures refers to functions carried out by a computer. Note that the controls exercised by the data processing department may be manual or based on other programmed procedures.

II FUNDAMENTAL CONCEPTS

A THE AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

1 Davis G.B - Auditing & EDP (1)

Davis G.B (1/110-112) defines controls in a computer environment as follows:

General System Controls

- | | |
|-------------------|--|
| Organisation | : deals with various functions in the data processing department |
| Documentation | : relates to program, system and other documentation |
| Hardware Controls | : cover hardware malfunction and error checks |

Specific Application Controls

- | | |
|---------------------------|---|
| Input and Output Controls | : cover control over input and output of data |
| Processing Controls | : cover control during processing of data |
| Audit Trail | : deals with forward or backward tracing of data. |

The model which highlights control points to prevent or detect errors is illustrated as follows:

Company Organisation, Management and Procedures

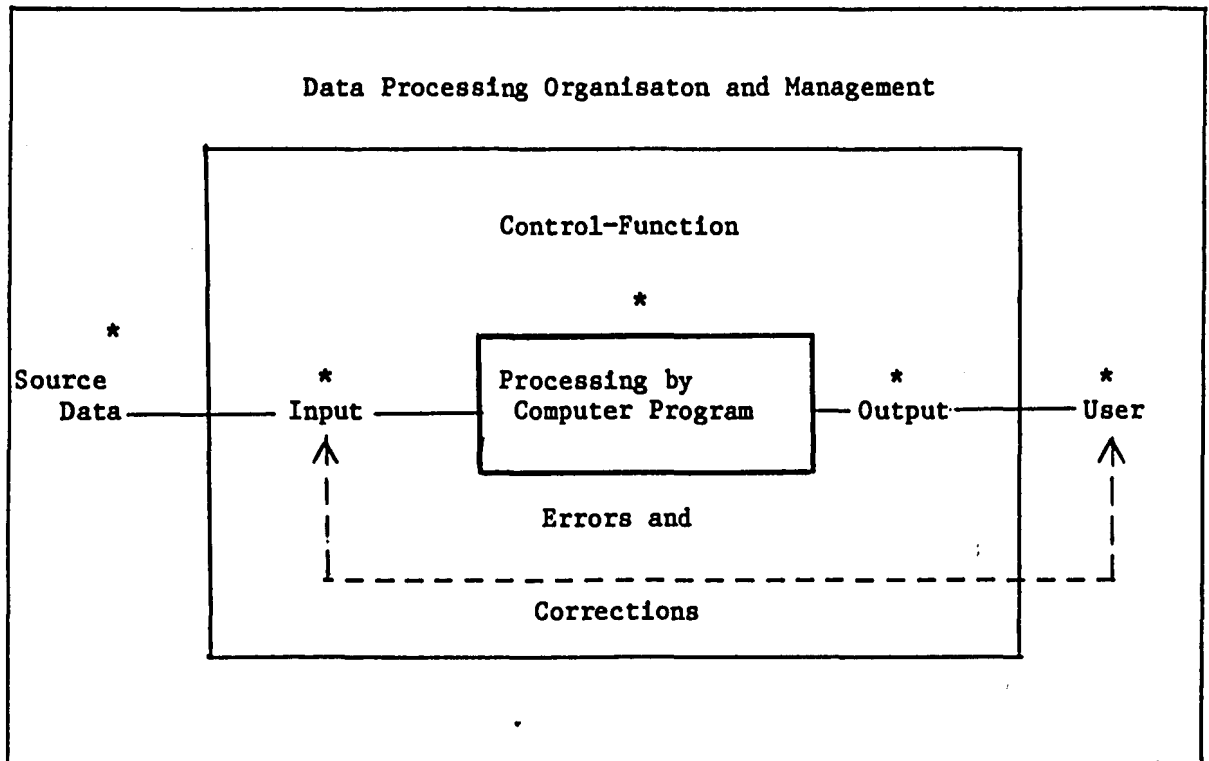


Fig 1. Control in a computer data processing system Davis G.B (1/110)

In terms of the basic definitions, general system controls and some processing controls relate to integrity controls while the remaining are application controls. The reason for classifying some processing controls as integrity controls is that they relate to the data processing department eg the computer operator may exercise some processing controls. Davis G.B.(1) contains no formal specification about the mapping of the various controls between each other. Mapping refers to the inter-relationship and impact of the various controls. Formal mapping is important as it provides details of the priorities, relative importance and position of controls. For example assuming there are no file safeguards but all the other controls are in place, would it mean there are inadequate controls? Alternatively could one rely on application controls to compensate for those weaknesses? Despite the lack of formal mapping a few interesting points are made:

Page 111 "There are programmed controls at only one of these control points" This refers to processing by computer program as set out in fig.1. "... but they make up only a part of the complete set of controls. It is important for the auditor to avoid viewing each control separately; he must view the entire set of controls which apply to an application as well as the organisational and management environment in which they are applied."

Page 209 "In systems using remote on-line input devices the problem of
- 210 authorisation may be more complex" and "Authorisation is programmed into the computer."

The above points are, however, made without any reference or guidance for applying them. For purposes of this literature survey they are important points as they suggest that:

- (a) The various controls do in fact map in some way;
- (b) Controls should be evaluated for the total system ie. the user and data processing component.
- (c) As the point of entry moves to the user eg. on-line systems, the traditional concepts of control could change. In fact the specific paragraph on page 209 can be interpreted to mean that the roles of applications and integrity controls can change ie. the authorisation of input may be "performed" by the computer - no longer a user.

2 The American Institute of Certified Public Accountants - Management Control and Audit of Advanced EDP Systems. (5)

The reference forms part of the Computer Services Guidelines series which is published by The AICPA. Its objective is therefore not to provide a model but rather to provide guidelines when dealing with specific issues, in this case Advanced EDP Systems. The intention in using this reference is to supplement the concepts in Davis G.B. (1) which have already been discussed. Technology has developed to the extent that systems classified as advanced systems when Davis G.B. (1) was written are today's norm. One need only consider current small business systems to see the rapid increase in technological complexity over the last six years. A specific illustration is the IBM PC/XT370 Personal computer which can be upgraded to 640k main memory, 4 megabytes virtual memory and has an operating system based on the mainframe VM (virtual machine) system.

The AICPA (5/11) defines features of modern systems which are considered necessary elements:

- (a) User identification. "The system should have the capacity to uniquely identify each of the specific persons using the system".
- (b) Request authorisation. "The system should be able to determine if the processing or information request of a user is authorised".

- (c) Process Integrity. "The system should be capable of controlling and processing all validated user requests in an appropriate time frame".
- (d) Activity Logging. "The system should be capable of recording all user activity such as the number of attempted logons request type, and the like, as well as recording information about the processes executed".

The underlying reasons for defining such requirements are fundamental to the very basic concepts of control:

- (a) Division of duties. The AICPA (5/7) states: "It is only through such an authorization system that the concept of segregation of functions can be maintained in an integrated system". Obviously the concept of user identification is a fundamental assumption as the absence of such a feature would make authorisation and hence division of duties impossible. Statements such as these have a significant impact on current control theory. Consider the traditional approach where one tended to consider application controls, including division of duties seperately from the integrity controls, including division of duties in the data processing department. The logical conclusion from saying that an authorisation system enforces division of duties is that the boundaries between which controls are pure application controls and those which are pure integrity control may be blurred and therefore one should examine the total system when evaluating controls ie. both the user component and the data processing component while bearing in mind that the distinction may often be unclear.

(b) Process Integrity. The AICPA (5/7) states: "Here again, system controls assume great importance and it behooves both management and auditors to assure themselves that such controls are designed into the systems and cannot be circumvented". In today's computer systems more and more routine procedures, including many of those traditionally used for control purposes, are being automated. Should a person be able to interfere with the normal functioning of the computer it may be possible to circumvent controls. As in the previous paragraph we conclude that the distinction of the boundaries between application controls and integrity controls has become blurred.

Although this reference did not provide a specific model to work from it has provided some interesting points on advanced EDP systems, which are today's norm. The most important point is the support it provides for the need to consider the total system when evaluating controls. Analysis of the various comments and suggestions provide the basis for reviewing the traditional concepts of division of duties and control procedures. Basically it involves the merging of controls which have always been regarded as purely application controls and integrity controls.

B THE INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES

3. Jenkins B and Pinkney A, An Audit Approach to Computers (2)

Jenkins and Pinkney (2) provides another perspective of controls in a computer environment. Although the formulation is somewhat different from Davis G.B. (1) there are distinct similarities. The model can be illustrated as follows:

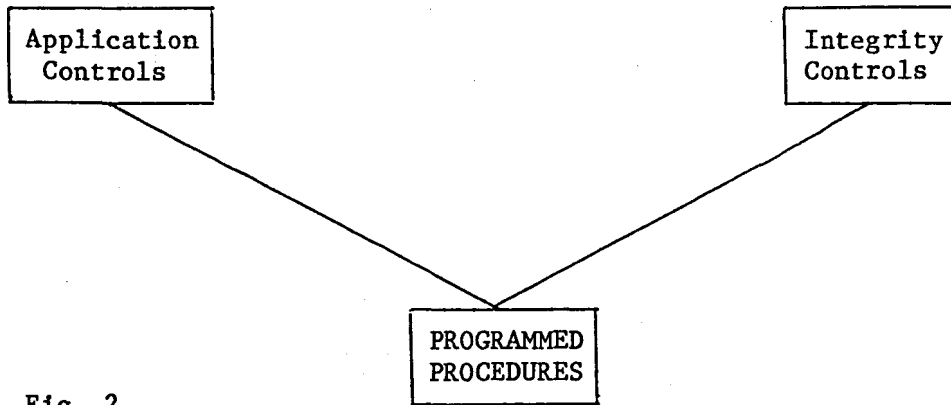


Fig. 2

Application controls cover input processing and output controls. The concept of authorisation and maintenance of files is also defined under the heading of application controls. Integrity controls on the other hand deal with controls over implementation and maintenance of application systems, security programs and data, computer operations and system software. A significant feature of the model is that it has a formalised interface between application controls (the user component) and integrity controls (the data processing component). Wherever the computer carries out a function which the user relies upon without rechecking it, this function is defined as a programmed procedure. The objective of integrity controls is to ensure that all programmed procedures are effectively implemented and subsequently continue to operate properly.

The interface or mapping is illustrated as follows:

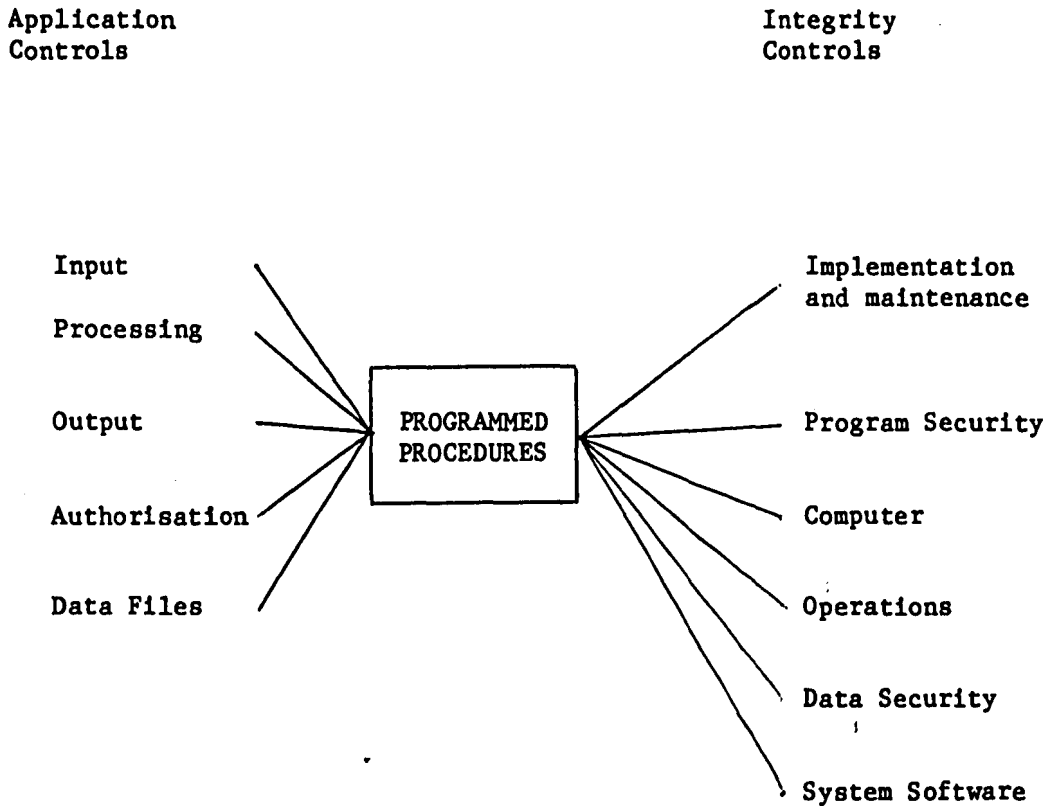


Fig. 3

In essence integrity controls cover all programmed procedures. Considered in terms of general control theory the interface is somewhat primitive: The main reason is that the mapping can only result in reliance on integrity controls if they are all in place. In other words if there are programmed procedures whose proper functioning is not assured by user controls then one can only rely on integrity controls if all the underlying areas are properly controlled ie implementation controls, program and data security, computer operations and system software. This interface, however, is significant as it is the only authoritative reference which provides this basis for a more formalised interaction between application and integrity controls.

C THE INSTITUTE OF INTERNAL AUDITORS

1. The Institute of Internal Auditors - Systems Auditability and Control- Central Practices (3)

The IIA (3/23-24) have a unique classification of application system and general controls which can be summarised as follows:

Application System controls

Transaction Origination	: governs the origination, approval and processing of source documents
Data Processing	
Transactions Entry	: deals with data entry, batch or otherwise
Data Communications	: governs the completeness and accuracy of data communications
Computer Processing	: covers accuracy and completeness of transaction processing
Data Storage and Retrieval	: deals with file controls including maintenance and security
Output Processing	: checking and balancing of output.

General Controls

Computer Service Center Controls	: deals with procedures within the data processing department which are not application specific. This includes division of duties.
Application System Development Controls	: covers development and maintenance of systems.

The inter-relationship of the various application system controls can be represented by fig. 4

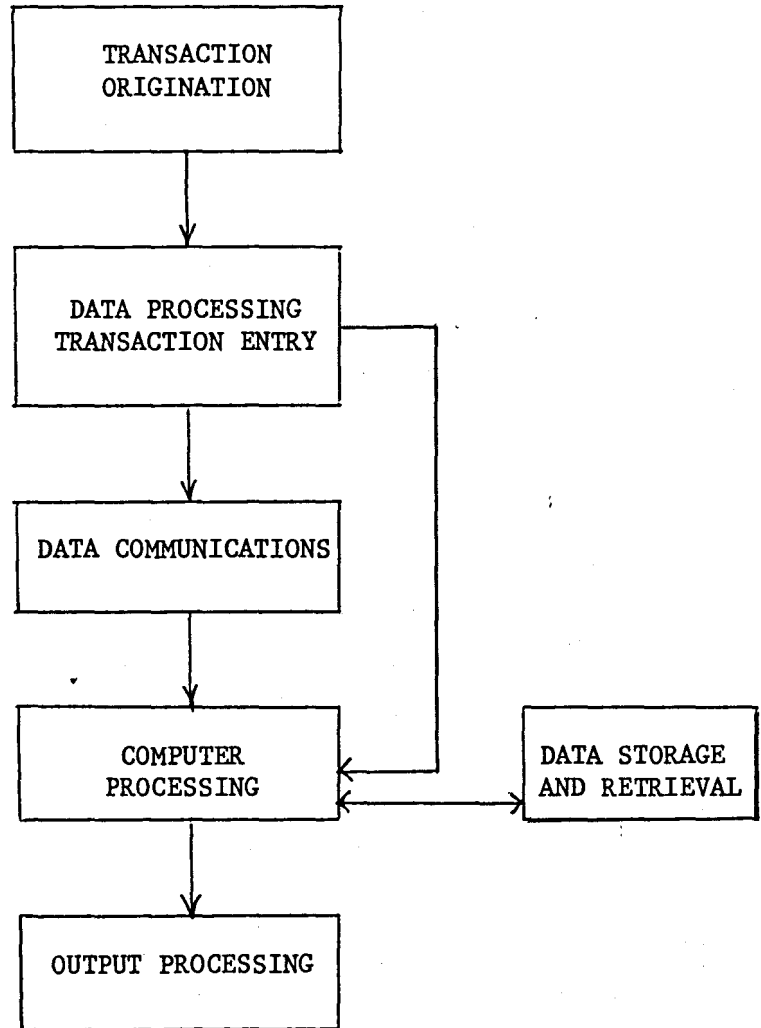


Fig. 4

There are a number of very interesting concepts which arise from an analysis of this approach.

- (a) A number of controls viz. some data communication and some data storage and retrieval controls which have been traditionally regarded as general or at least not application specific are evaluated for each application. They can be classified as application specific controls. This approach suggests that the auditor can evaluate controls over individual transactions from inception through subsequent processing to final output and consider the user and data processing component of a system. In addition aspects dealing with terminal security, data file security, computer operators and system software are also covered on an application specific basis.
- (b) The areas, which in the writer's opinion, are not dealt with properly are authorisation of transactions and division of duties. Although mechanisms which may provide authorisation are described within each application control type, there is no formalised theory for dealing with authorisation. It leaves out important questions about the effectiveness and timing of authorisation. In fact by having controls down to a specific transaction level it appears that the total system perspective is not maintained. Division of duties is regarded as a general control and the definition the IIA (3/95) gives, the objectives of division of duties are to provide "... adequate separation of duties both within the data processing department and between data processing and user areas" and "... automated program controls to control on-line systems". It is of interest to note that no reason is given for classifying division of duties as a general control which implies that it spans multiple applications.

(c) The way in which this model has been defined allows for controls within control types such as transactions origination and data communications. Within each type various areas such as document authorisation and document retention in the case of transaction origination are defined. Whilst a very exhaustive list of control types and their underlying areas are defined it is difficult to determine under which circumstances the various controls will be necessary. One example is authorisation of source documents. The way in which transaction origination is defined (The IIA 3/51) it is unclear to what extent authorisation of source documents is necessary. One can think of a number of cases eg. cheque receipts where source documents need not be authorised. It would seem that an approach such as this which is not driven by control objectives that need to be met, could lead to overcontrolled situations as controls are implemented because they are necessary in accordance with a checklist rather than because they meet some control objective.

D THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS

1. The Canadian Institute of Chartered Accountants - Computer Control Guidelines (8)

The CICA (8/3) introduce a very sophisticated control model with a high degree of interaction between the various types of controls.

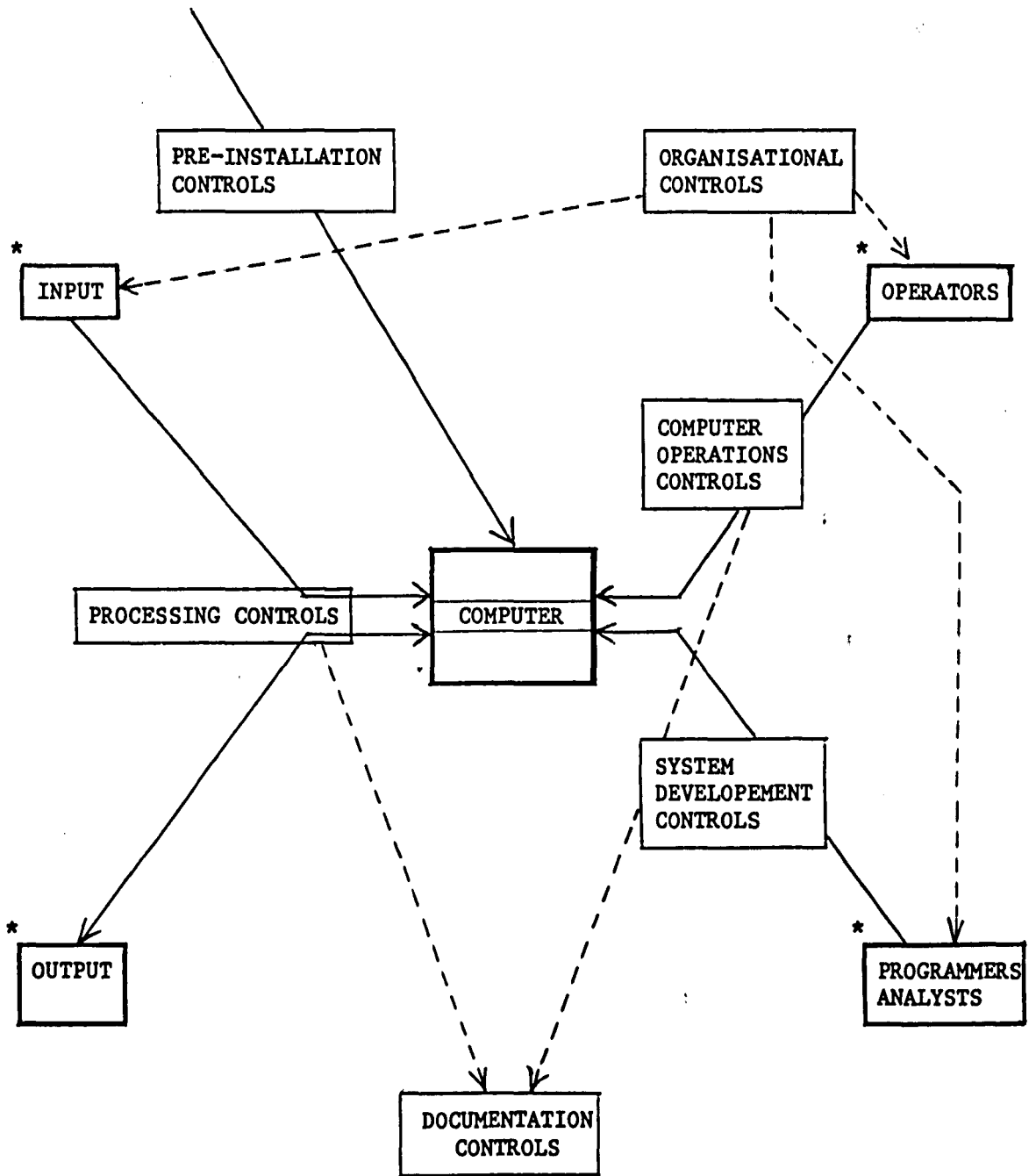


Fig. 5

* = Denotes functional areas while the others denote control areas.

The terminology which is used is the same as much of the previous literature and no further explanations are considered necessary. Each type of control in the model (see fig. 5) is defined in terms of control objectives that need to be achieved. The CICA (8/5) state that "These are the control standards which the Study Group believes it is necessary for a computer system to meet" and "Under each control objective there may be anywhere from one to ten minimum standards". Prima facie analysis suggests that the whole approach is very rigid in structure although a degree of interaction between various control types is acknowledged (The CICA 8/2). Of major significance is the absence of the motivation for having the various control objectives within each control type. In practice controls implemented simply for the sake of having them do not work effectively and generally speaking, it may often be difficult to justify their necessity. Quite often the absence of a particular control is unlikely to lead to error or fraud as another control, which may be a different control type, may compensate for this specific weakness.

It is unclear as to how this phenomena can be dealt with in the framework provided despite the fact that a high degree of interaction of control types is acknowledged.

No other points which would assist in researching the interaction between application and integrity controls as defined in the objectives, were found.

III ANALYSIS OF REFERENCES

1 Comparative Analysis

In the previous section the basic model of each reference was defined using the terminology given in each case. To do a detailed analysis it was found necessary to classify the various controls used in each reference in terms of the definitions given in section I(D). The key to this classification is that application controls are those exercised by the users while integrity controls are those exercised by the data processing department either manually or based on programmed procedures.

The table below sets out how each reference views controls on the application - integrity control comparative basis defined previously.

Reference	Component	Application Controls	Integrity Controls
Davis G.B (1)	General System Controls		x
	Specific Application Controls		
	- Input and Output Controls	x	x
	- Processing Controls	x	x
	- Audit Trails	Not a control as such	
Jenkins B & Pinkney A (2)	Application Controls	x	
	Integrity Controls		x
The IIA (3)	Application System Controls		
	- Transaction Origination	x	
	- Data Processing Transaction Entry	x	x
	- Data Communications		x
	- Computer Processing	x	x
	- Data Storage and Retrieval		x
	- Output Processing	x	x
	General Controls		x
The CICA (8)	Pre-Installation Controls		x
	Organizational Controls	x	x
	Development Controls		x
	Operations Controls		x
	Processing Controls	x	x
	Documentation Controls		x

A number of important conclusions can be made from this table despite the fact that the definitions used at this stage of the dissertation are somewhat informal:

- (a) All the control models acknowledge application and integrity controls within a computer system. It is therefore a logical conclusion that all computer systems have both a user component and a data processing component. Although this may seem a trivial statement it proves that the data processing component of a computer system is an integral part of a computer system and cannot be ignored as is quite often the situation in practice.

- (b) There are a number of control types within each model that relate to both application and integrity control components. In these circumstances an application control may:
- (i) complement a specific integrity control or vice versa;
 - (ii) depend on a specific integrity control;
 - (iii) compensate for a lack of a specific integrity control.

This degree of interaction between the two suggests that there may be a formal relationship between application and integrity controls.

- (c) There is little consensus among the various authors and/or professional bodies about the actual interfacing of control types and it is of interest to note that none of the references discuss the actual need for all the underlying control types. Instead the approach adopted tends to be a "have to have" philosophy with little regard for a comprehensive theory which defines:

- (i) which controls are essential;
- (ii) which controls complement each other;
- (iii) which controls can compensate for each other;
- (v) which controls depend on each other;
- (vi) circumstances when presence of certain controls are essential.

- (d) Although each model acknowledges the existence, dependency and interaction of application and integrity controls, albeit it using different terminology, there are many differences between the level at which the control types interact. The interaction can occur at the transaction, application program, application system (a number of related application programs) or data processing department levels.

For example Jenkins B and Pinkney A (2) define programmed procedures at transaction level but integrity controls cover these as a whole. The IIA (3/23) on the other hand attempts to define most of the controls on an application basis viz. application system controls.

2 Conclusion

Before arriving at a conclusion it is necessary to recap and determine what basis or guidance for research the literature survey can provide. The previous section has indicated that:

- (a) There is lack of consensus between the various references for the nature, scope and need for the various application and integrity controls.
- (b) The basic theory stating why various controls are required is absent or not obvious from the references.
- (c) The various models are largely incompatible in the sense that the level of interfacing between the control types vary from non existent eg Davis G.B (1) where it is simply mentioned as a point, to the IIA (3) where controls are interfaced by viewing the flow of transaction through a system. Despite many references to the evaluation of a total system it is not possible to determine:
 - (i) the circumstances in which certain controls are essential;
 - (ii) how they depend on each other;
 - (iii) how they interact.

For a research paper of this nature it is only possible to arrive at the conclusion that it may be necessary to question the very basic fundamentals of controls in a computer environment. This statement is not intended as a criticism of the references, in fact all of them make some very important theoretical points. Of greater significance are points suggesting the evaluation of controls for the total system and those dealing with authorisation and division of duties in a computer system. A detailed search for a reference dealing with the theory which is lacking from the authoritative references was done to no avail. It would appear that controls are only intuitively understood in a computer environment and that to obtain a proper synthesis of controls it is necessary to begin with the fundamental concepts and attempt to define the basic control theory in a more formal way. Only then i.e. when more about controls is understood, can an attempt be made to evaluate their interaction. The literature survey has however provided a great deal of information which can be used in this dissertation. The views are authoritative and many provide valuable insight into the survey of application controls.

Although the literature survey did not satisfy the initial objectives completely, a great deal of guidance for control theory and ultimate objectives was discovered which will assist with further research.

IV BIBLIOGRAPHY

- 1 Davis, G.B. Auditing & EDP, 1978 The American Institute of Certified Public Accountants, Inc.
- 2 Jenkins, B. and Pinkney, A., An Audit Approach to Computers, 1975, The Institute of Chartered Accountants in England and Wales.
- 3 Stanford Research Institute for The Institute of Internal Auditors, Systems Auditability & Control - Control Practices, 1977, The Institute of Internal Auditors.

- 4 **Stanford Research Institute for The Institute of Internal Auditors, Systems Auditability & Control - Audit Practices, 1977, The Institute of Internal Auditors.**

- 5 **The American Institute of Certified Public Accountants - Computer Services Guidelines, Management, Control and Audit of Advanced EDP systems, 1977, American Institute of Certified Public Accountants, Inc.**

- 6 **The American Institute of Certified Public Accountants - Computer Serviced Guidelines, Controls over Using and Changing Computer Programs, 1979, American Institue of Certified Public Accountants, Inc.**

- 7 **The Canadian Institute of Chartered Accountants - Computer Audit Guidelines, 1975 The Canadian Institute of Chartered Accounts.**

- 8 **The Canadian Institute of Chartered Accountants - Computer control Guidelines, 1973 The Canadian Institute of Chartered Accountants.**

COMPUTER CONTROL HYPOTHESIS - CONCEPTS AND DEFINITIONS

It was concluded in the literature survey that traditional control methodologies are inadequate to describe modern day computer systems as the data processing component cannot be divorced from the user component. One example is an on-line real time system where the traditional role of the computer operator is often migrated to the users who run and control their own systems. The literature survey was useful in that most professional bodies agreed that one should examine the total system and that interaction between control types does in fact exist.

To formulate control theory which allows for a formal interface between application and integrity controls it is necessary to re-examine the fundamental concepts of internal control and to derive a hypothetical model which complies with those concepts and secondly, which describes this interface. The objective of this chapter is to describe the hypothesis in more formal terms and then proceed with a description of an interface in the following chapter. The following headings have been used:-

I DEFINITIONS

II PROPOSITIONS

III POSTULATE

IV HYPOTHETICAL MODEL

I DEFINITIONS

- a. Application Software
 - b. System software
 - c. Transient versus Stored Data
 - d. Programmed Procedures
 - e. Application Controls
 - f. Integrity Controls
 - g. Data Path
 - h. Task Integrity
 - i. Data Integrity
-
- (a) Application software includes internally developed or purchased software which is used to process a specific part of an organisations data. Examples are purchases, sales and payroll applications.
 - (b) System software includes internally developed or purchased software which can be used by more than one application system. System software is therefore usually generic in nature and is mostly used to perform some form of service which the application systems need to function properly. Examples are operating systems, teleprocessing monitors, data base management systems, compilers and utility programs.
 - (c) Transient data is data in the process of being initiated and input into an application system, processed by the computer, written to data files or being output. Stored data refers to data which is stored on a data file and remains static for a period of time. This would include all transaction, master and temporary files in an application system.
 - (d) Programmed procedures are functions performed by the computer to perform routine procedures or as a basis for exercising a control.

- (e) Application Controls are those controls exercised by users of application software over a specific system's transient and stored data. Users may rely on programmed procedures for control purposes.
- (f) Integrity Controls are those manual, system software or application software based controls which are exercised or directed by the data processing function in an organisation over transient and stored data. Integrity Controls are often transparent to users and are often based on very complex programmed procedures.
- (g) The data path of an application system is defined as the user departments, data processing department, application software and system software through which data relating to a specific application would have to pass to become stored data or to produce output. It therefore covers the complete or total system i.e. both the user and data processing components of the system.
- (h) Task integrity refers to assurance that data within a data path is not unintentionally corrupted at any stage while transient.
- (i) Data integrity refers to assurance that stored data is not unintentionally corrupted.

II PROPOSITIONS

The first two propositions are based on statements issued by the South African Institute of Chartered Accountants and deal with a number of fundamental issues:

- a. Basic principles of Internal Control - see (a) below.
- b. Purpose of the Auditor's Study - see (b) below.
 - (a) Statement AU230 (10) - Internal Control, paragraph .07 states: "The basic principles of internal control are independent of the method used to process accounting data. However, the procedures followed in relation to computer applications may require additional consideration."

- (b) The purpose of the auditor's study of internal control is twofold: Firstly as a basis for obtaining assurance of the accuracy and reliability of his clients accounting records. This is in accordance with accepted audit practice - paragraph .09 of Statement AU230 (10) dealing with Internal Control. Not always so obvious is the auditors duty to detect fraud and error if material. Internal Control is a preventative and/or detective safeguard against intentional and unintentional error as well as fraud. Although the auditor has a limited duty to detect all fraud, an understanding and evaluation of internal control is necessary to determine the risk of error and fraud. Obviously the better the internal controls, the lower the risk of fraud.

From the above propositions a number of interesting derivative propositions can be made:

- c. Complete, accurate and reliable financial records - see (c) below.
- d. Intentional error and fraud related controls - see (d) below.

(c) In order to obtain assurance that accounting records are accurate and reliable it is necessary to ensure that:

- (i) all underlying transactions have been brought to account. This is defined as completeness.
- (ii) each underlying transaction's data is correctly reflected, i.e. without error. This is defined as accuracy.
- (iii) the underlying transactions are valid in terms of corporate policies. The term valid does not cover fraud. In fact a fraudulent transaction may sometimes be a valid transaction. This is a matter of definition only, but for the purpose of this dissertation a distinction is made between accurate and reliable records and whether fraudulent but valid transactions are included.

Paragraphs (i) to (iii) above cover data in the form of transactions, both at the transient and stored stages.

- (d) Controls which safeguard against intentional error and fraud are often different and more stringent than those which ensure accurate and reliable accounting records. This may seem a contradiction in terms, but it is in fact quite logical. For example it is fairly easy to ensure that all transactions are accounted for accurately, including fraudulent ones. It is much more difficult to prevent or detect a fictitious or fraudulent transaction. To achieve this requires procedures for authorising transactions, checking underlying documents performing other checks and segregation of duties. The concept of accurate and reliable accounting records and prevention or detection of intentional error and fraud are not necessarily synonymous and a control methodology needs to address this issue as such.

Having differentiated between fraud, intentional errors and unintentional errors a number of important postulates can be made which affect traditional computer control theory as follows:-

Segregation of duties - see (e) below.

Responsible officials and authorisation - see (f) below.

Data processing organisation - see (g) below.

- (e) Segregation of duties is primarily a safeguard against intentional error and fraud. The fundamental concept is that one person should not have access to the records, the underlying asset and reconciliation of assets and records. Division of duties is, however, also a control mechanism to ensure that management policies relating to transactions are adhered to.

- (f) A person who has the authority to authorize transactions, adjustments or journals is usually in a position to conceal error and fraud. Such a person falls outside the normal division of duties concept as he is able to bypass much of the system of internal control. It is necessary to consider such a person a responsible official of the concern.
- (g) Traditionally segregation of duties between users and the data processing function have been regarded as separate issues. Division of duties should, however, logically extend to the data processing department in the sense that certain persons there may have access to both the records and the assets. In principle, the segregation of duties issue applies to a functional area, for example sales, and embraces both the user and data processing departments. Therefore, as with data paths, the total system is covered.

III POSTULATE

The following control objectives are overall control objectives and cover or span both application and integrity controls:

- (a) Completeness and accuracy controls are required over transient data throughout the data path in order to ensure task integrity.
- (b) Completeness and accuracy controls are required over stored data to ensure data integrity.
- (c) Controls are necessary to ensure the validity of transient data or changes to stored data.
- (d) Controls are necessary to safeguard against intentional error and fraud.

Application and integrity controls can be regarded as convenient ways of classifying the techniques that can be used to achieve the above control objectives. It may therefore be possible to define corresponding application and integrity control techniques each of which could achieve a control objective or can be combined to achieve a control.

IV HYPOTHETICAL MODEL

(a) Description

Based on the definitions, propositions and postulates it is possible to describe a hypothetical control model which complies with the criteria presented above:

- (i) The data path forms the nucleus of the model which is in line with the definitions previously established.
- (ii) Ultimately the auditor wants assurance about the completeness, accuracy and reliability of the accounting records and the risk of intentional error and fraud. The control objectives cover these on the basis that both application and integrity controls are spanned thus forming the base from which the auditor can evaluate the controls.
- (iii) Application and Integrity Controls do not each have their own unique control objectives, but provide a useful classification for control techniques. Each technique, however, has criteria which determines whether it has been properly implemented.
- (iv) The model is flexible and each component of the data path can be used as a basis for control. Generally speaking users exercise application controls although under certain circumstances they could exercise integrity controls. It is maintained that under these circumstances the user department assumes data processing functions and therefore certain integrity controls are necessary. Examples of such circumstances are end-user programming and users running programs from terminals.
- (v) Integrity controls are usually exercised by the data processing function, which includes the data processing department and users performing functions such as those described in the previous paragraph.

(b) The interface between application and integrity controls.

Because application and integrity controls are simply ways of classifying control techniques in terms of the organisation functions viz users and data processing it means that the interface is such that:

- (i) Application controls and integrity controls supplement or complement each other. It means that control can be viewed as a combination of application and integrity controls; and,
- (ii) Certain application controls and integrity controls can be substituted for one another.
- (iii) There is only a limited number of techniques in each case. This is significant as it is considered impossible to define a generic interface between application and integrity controls. This is evident from the problems encountered in the literature where models were defined using control objectives at the application/integrity control level.

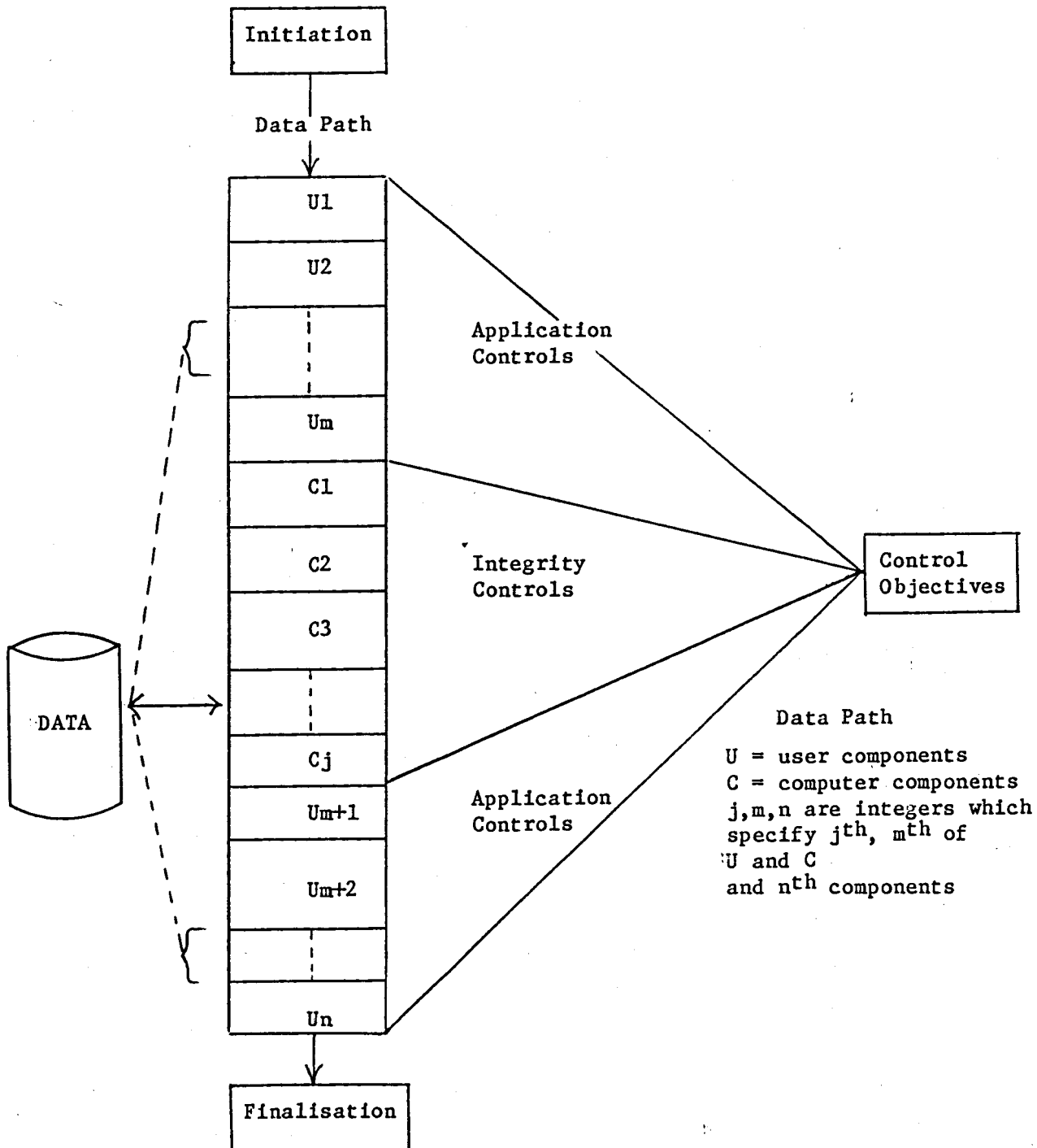
The detailed specification of an interface is presented in a following section.

V CONCLUSION

A hypothesis has been derived on the basis that internal control concepts do not change in a computer environment. It is only the new areas they introduce that need to be considered. To comply with this theory a number of overall control objectives have been defined with application and integrity controls simply being convenient ways of classifying control techniques. Another important concept is the separation of controls which ensure accurate and reliable financial records versus those which safeguard against intentional error and fraud. The reason for doing this is that fraud related controls are quite often very different from those which ensure accurate and reliable accounting records. It is possible at this stage to define an interface for application controls and integrity and then prove that the hypothesis is sound and practicable.

HYPOTHETICAL CONTROL MODEL

Stored Data Transient Data



COMPUTER CONTROL HYPOTHESIS - INTERFACING APPLICATION AND INTEGRITY CONTROLS

To determine how application and integrity controls inter-relate it is necessary to have a precise definition of the term control. For purposes of this dissertation a definition needs to be derived which will match the hypothesis or control model described previously and a more detailed hypothesis for interfacing application and integrity needs to be developed. The following headings are used:

I DEFINITION OF CONTROL

II THE INTERFACE BETWEEN APPLICATION AND INTEGRITY CONTROLS

III SUMMARY

I DEFINITION OF CONTROL

A control can be defined as a check to ensure that certain conditions have been met and that exceptions if any are followed up. To achieve this it must comply with the following rules:

(a) There must be a routine procedure or procedures for :

(i) checking conditions

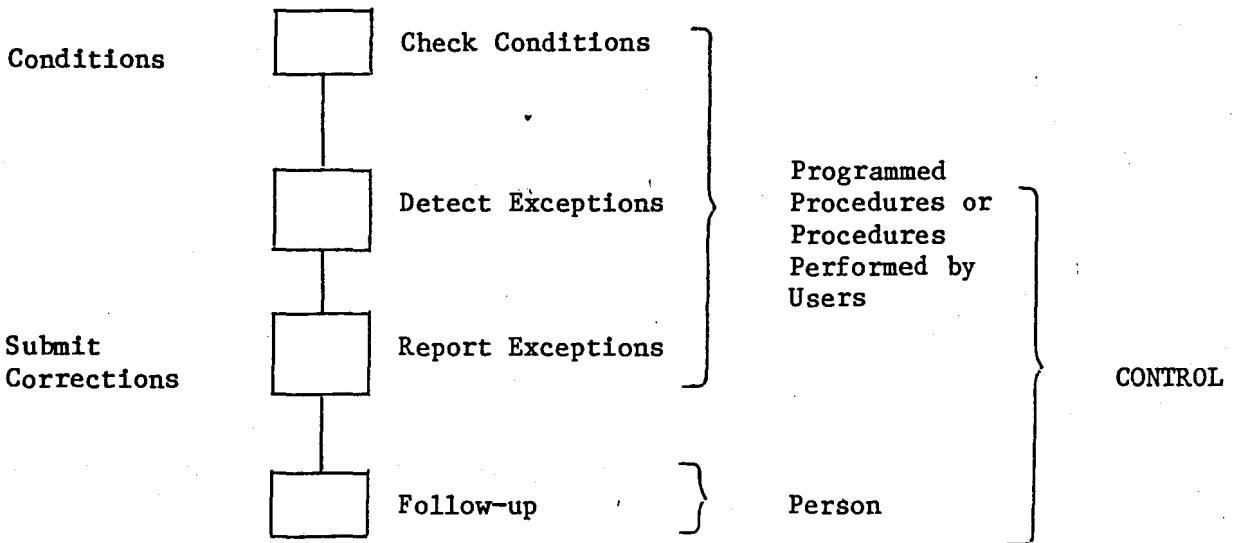
(ii) detecting exceptions

(iii) reporting the exceptions

(b) In addition procedures, not necessarily routine in nature, must exist to follow-up the reported exceptions and initiate corrections.

The absence of any component implies, per definition, that the control is inadequate and cannot be relied on to function properly. Effectively it means there is no control. This definition has a significant implication as a control cannot be "built" into the computer as the follow-up component has to be done by a human. Proof of this argument is the fact that unless someone follows up computer reported exceptions the whole exercise proves meaningless as errors are not corrected.

Consequently it is concluded that although a control cannot be built into the computer, the computer can be used as a basis for exercising control as it performs programmed procedures which can comply with part (a) of the control definition; the follow-up component, at least based on current technology, has to be done by a person. This process can be illustrated as follows:-



It is important to note that this theory complies with scientific open and closed loop control theory which represent the scientific models which are used in areas such as process control. In the audit control model described above the human operator is still an integral part as technology is not sophisticated enough to follow up the random nature of exceptions encountered in a typical business environment. The abovementioned definition of control will be implied with the use of the term throughout the following sections of this dissertation.

II THE INTERFACE BETWEEN APPLICATION AND INTEGRITY CONTROLS

To ensure consistency with the hypothesis two aspects are of prime importance.

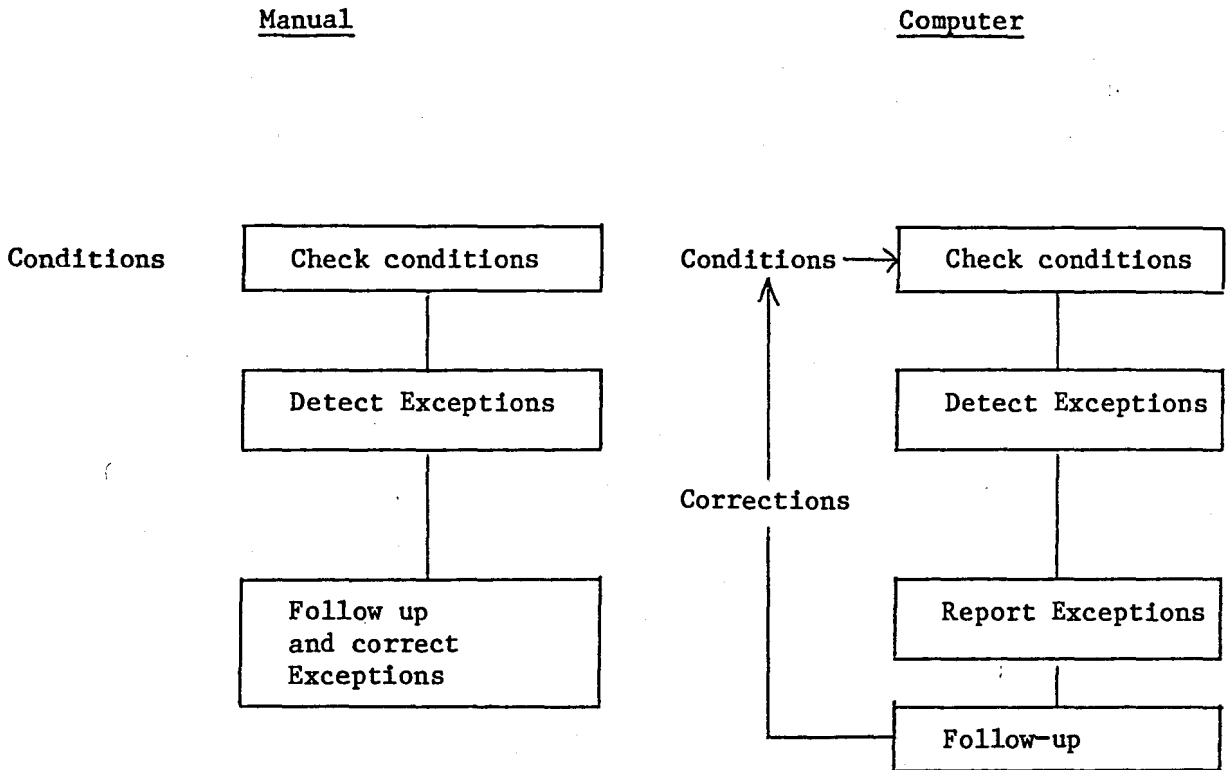
- (a) Application and Integrity Controls are simply ways of classifying alternative control techniques.
- (b) The definition of control requires a human operator component in all cases. It can however be an application software user, also termed user, or data processing personnel.

This section is presented in terms of the overall control objectives which have been previously defined as a postulate :

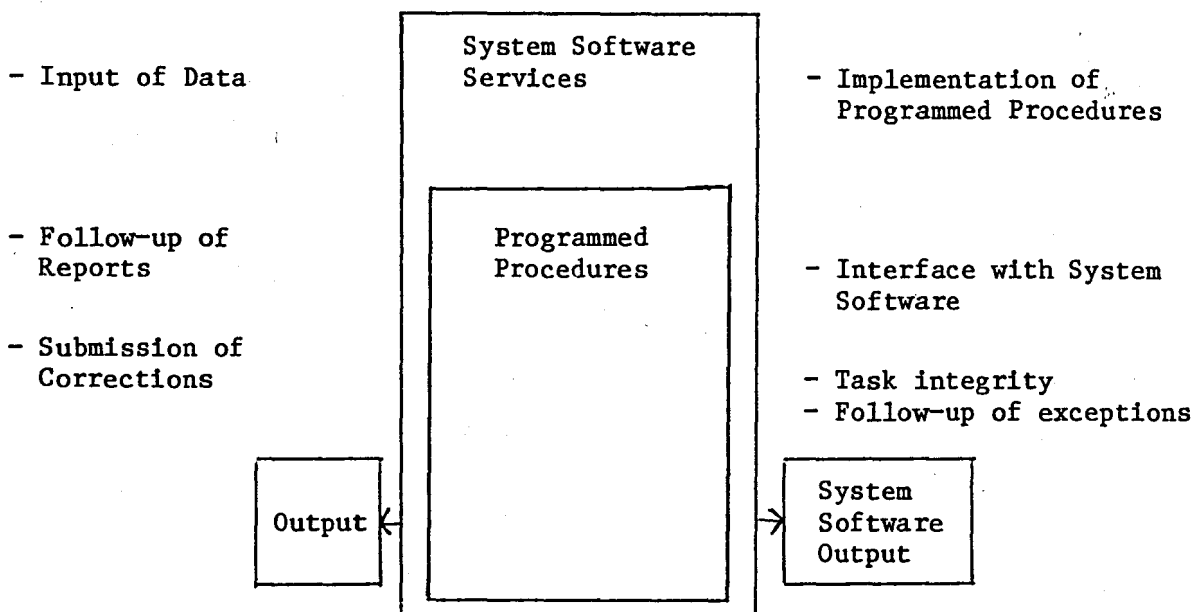
- A. COMPLETENESS AND ACCURACY OVER TRANSIENT DATA
- B. COMPLETENESS AND ACCURACY OVER STORED DATA
- C. VALIDITY OF TRANSIENT DATA AND CHANGES TO STORED DATA
- D. SAFEGUARD AGAINST INTENTIONAL ERRORS AND FRAUD

A. COMPLETENESS AND ACCURACY OVER TRANSIENT DATA (Task Integrity)

Control in a manual system is relatively simple as the person doing or checking the work has access to all the underlying working papers and records. Using the diagram previously introduced to illustrate a control, the following comparison can be derived.



Manual systems are such that a formal reporting and separate follow-up and correction component is not normally necessary as the manual records are simply corrected. The reason for requiring a more elaborate approach in a computer system is that the data path defined in the previous section, has an additional component, the computer. Computers cannot be viewed as a black box as each computer system may contain multiple components such as an operating system, teleprocessing monitor or a data base management system. Quite often the computer is relied upon to perform a programmed procedure without the realisation that there are others which are transparent to the user and which are also executed. Most of these relate to system software services used by application software. An evaluation of the interface between application and integrity controls would therefore have to take this into account. This relationship can be represented as follows:-

Application ControlsComputerIntegrity Controls

Update of Data File/s where
Applicable

In essence the proposed hypothesis suggests that :-

- (a) Current technology does not permit direct substitution between application and integrity controls to achieve completeness and accuracy of transient data.
- (b) The best possible alternative is to automate the routine procedures (programmed procedures) but still have a user component of the system; the follow-up of exceptions.
- (c) Controls over programmed procedures can be achieved by either re-performance by a user or reliance on integrity controls as shown in the diagram. Having users re-perform the hundreds of programmed procedures in an on-line system is not considered practicable in most cases today as all the edit checks, exceptions and calculations would have to be included.

B. COMPLETENESS AND ACCURACY OVER STORED DATA (Data Integrity)

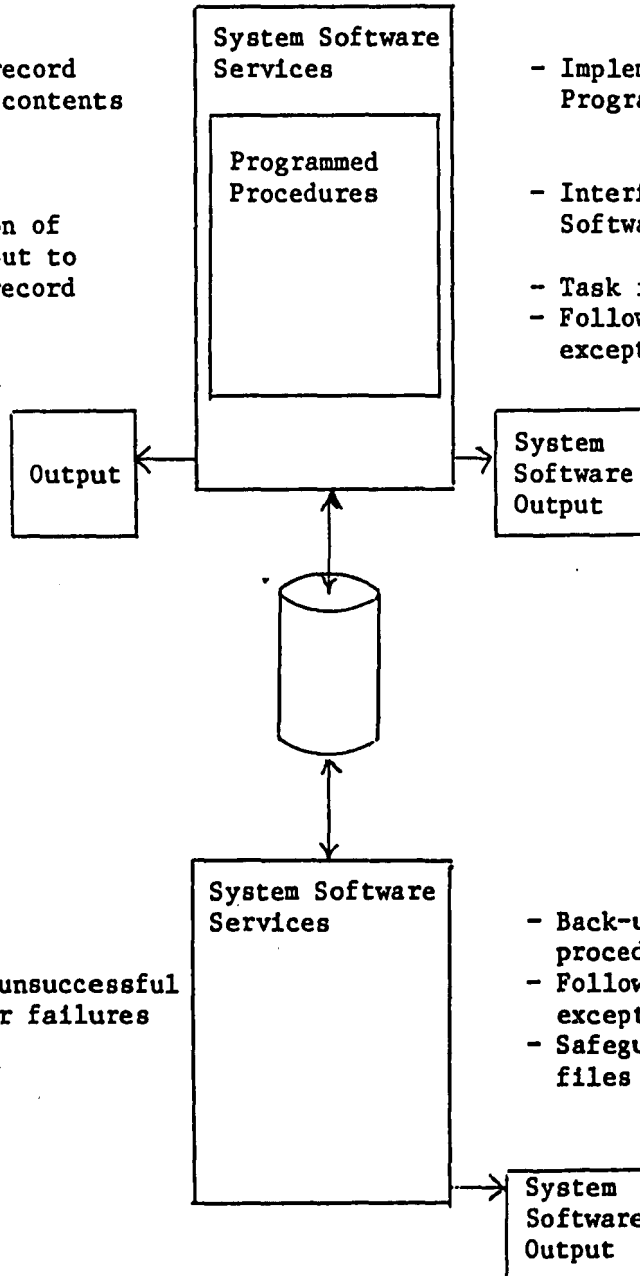
Once data has been written to a data file, or data files, it is essential that controls are present to ensure completeness and accuracy of the stored data. Changes introduced as a result of intentional error and fraud are excluded from this section and is dealt with as a separate issue. Under normal circumstances events such as computer failures and inadequate programmed procedures would be the main cause of errors under this control objective. Traditional controls include control accounts, reconciliation of file totals and one-for-one checks of file contents. Synonomous with controls under this heading is the term data integrity defined previously as assurance that stored data is not corrupted unintentionally. To define the interface between application and integrity controls it is necessary to determine the mechanisms available to ensure data integrity. Examples of such mechanisms are the sophisticated back-up and recovery techniques which are often an integral component of the file management function of the operating or data base system. In addition the safeguarding of files, including back-up copies, against accidental deletion becomes essential as a mechanism to preserve overall data integrity. The reports of system exceptions provide the basis for relying on integrity controls to assure data integrity.

The hypothesis of the interface as it relates to data integrity is represented as follows :-

Application Controls

- Independant record of data file contents
- Reconciliation of Computer Output to Independant record
- Follow up of discrepancies

Computer



- Follow-up of unsuccessful recovery after failures

Integrity Controls

- Implementation of Programmed Procedures
- Interface with System Software
- Task integrity
- Follow up of system exceptions
- Back-up and recovery procedures
- Follow-up of system exceptions
- Safeguarding of back-up files

It is important to note that :-

- (i) Current technology permits substitution of application and integrity controls as presented above. In the event of the integrity controls being adequate it is possible to have adequate data integrity without elaborate application controls such as one-for-one checking of file contents.

C. VALIDITY OF TRANSIENT DATA AND CHANGES TO STORED DATA

The objective of validity is to ensure that management policies regarding processing of data and changes to stored data are complied with. More specifically the policies normally cover :-

- (a) Criteria for processing specific transactions which include the use of standing data. Examples are invoice pricing and purchasing criteria. Management for example, approves a price list which is incorporated into the computer system or specify that more than one quote needs to be obtained for purchases.
- (b) The persons who are permitted to process transactions and the types of transactions permitted, including those which change stored data. A concept of "authorised to process" arises from this section. Note that a fraudulent transaction processed by a person authorised to process it remains a valid transaction albeit fraudulent. This fraud versus reliable records issue has already been covered in the previous section. Controls to ensure that valid transactions are not fraudulent would assume some form of supervision and authorisation and would vest with the user as an application control. Fraud and intentional error are however, covered separately later in this section.

The traditional application controls which ensure validity of transactions include checking the work of others, approval of transactions, division of duties and supervision. As in the previous paragraphs the diagram presented below describes the hypothesis. It is based on a postulate that modern system software features which restrict the capabilities of users can enforce some of the above concepts. Note the distinction between approval and authorisation. Approval ensures transactions comply with management policies while authorisation is orientated towards fraud and intentional error. The implications are that approval can be incorporated as programmed procedures with, of course, the user following up exceptions.

Application controls

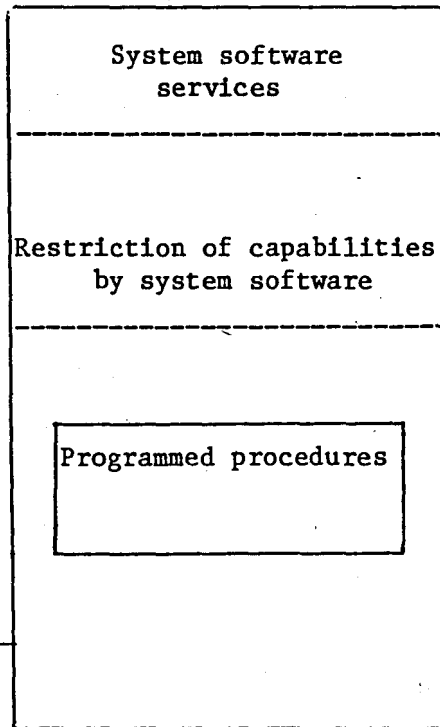
Computer

Integrity controls

Approval/Authorisation

Input of data

Follow up of reports



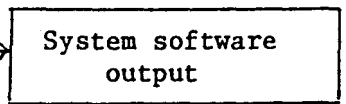
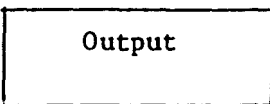
Implementation of programmed procedures

Implementation of "Restriction of capabilities".

Interface with system software

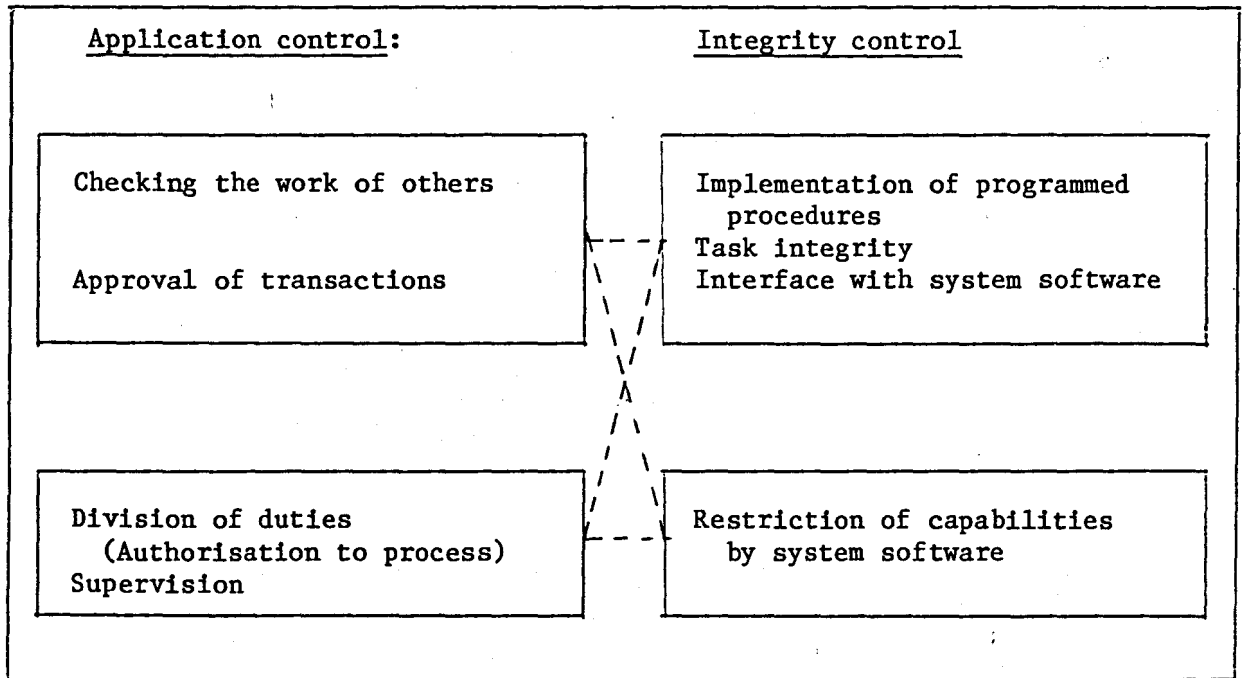
Task integrity

Follow up of system exceptions.



Update of data files

Below is a more detailed mapping of the application and integrity control techniques. Under this control objective there is a high degree of substitution whereby integrity controls and application controls can be interchanged while providing the same degree of control.



The following points are considered significant:-

- (a) Current technology permits a degree of substitution between the control types for this control objective.
- (b) The traditional concepts of approval and supervision can be substituted by integrity controls which monitor the activities of the users while using the computer. A concept of using technology to control technology is therefore present.
- (c) There is always the alternative choice of getting the users to re-check and approve all activities thus using humans to control technology. This is considered impracticable in a large computer environment.

D. SAFEGUARD AGAINST INTENTIONAL ERRORS AND FRAUD

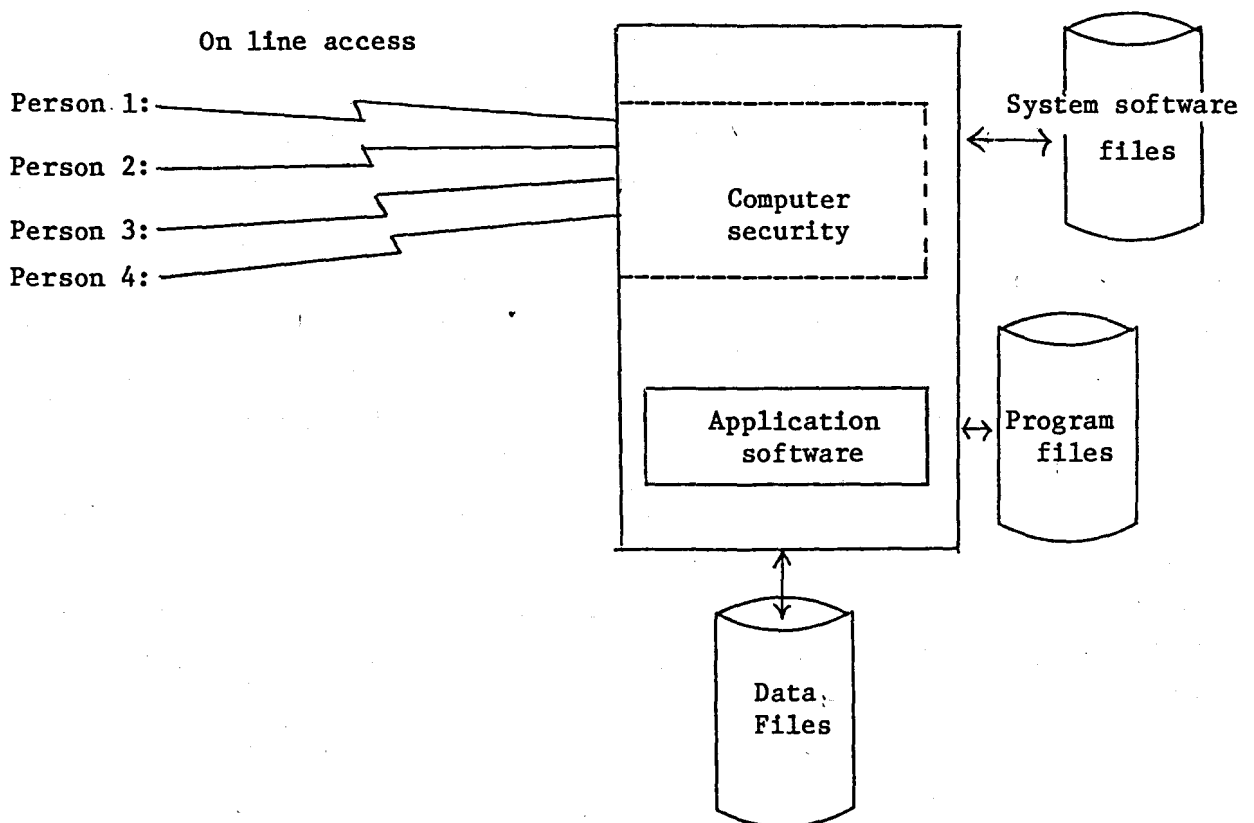
One of the most complex issues in computer auditing is that of fraud and intentional error. It covers the safeguard against intentional errors and fraud by both the users and data processing personnel in an organisation. Traditional controls to prevent and/or detect fraud are:-

- (a) Division of duties.
- (b) Authorisation of transactions and adjustments to accounting records.
- (c) Separate records of assets and accounting for assets. The most typical is the various subsidiary ledgers represented by control accounts in a general ledger.

The first generations of computers had little effect on these concepts as all the data processing activities were divorced from the user departments. In most instances the application controls, mainly batching, also spanned the computer element and relatively few problems arose except preventing access to production programs and data by data processing personnel. Physical procedures such as authorising jobs submitted in card or tape form were adequate controls. It is obvious that little change in the area of fraud and intentional error safeguards were necessary.

In a modern computer on-line system division of duties and the whole traditional concept of internal control are compromised with an increased risk of intentional error and fraud. For purposes of this dissertation it is assumed that computer security can be implemented in such a way that unauthorised access to programs and data can be prevented or at worst, detected and that the capabilities of every person who has access to the computer system can be restricted. Exactly how division of duties would work in such an environment falls outside the scope of this dissertation as it involves an extensive examination of fraud, error, authorisation, division of duties and independent records.

Some of these issues have already been raised in the previous section with the conclusion that division of duties for example, needs to span the total system and is not limited to separate structures for user and data processing departments. This implies interfacing and integrating traditional division of duties in all areas of an organisation, determining which transactions require authorisation and defining how computers permit supervision. As a result of the complex issues involved a very detailed hypothesis is not presented. The following diagram does however describe a hypothetical outline.



The area defined as computer security provides a degree of substitution between application and integrity controls. The traditional theory of division of duties is inadequate because:-

- (a) A user invoking processing from a terminal is assuming some of the duties traditionally carried out by computer operators.
- (b) The current tendency to permit end-user programming from user terminals implies that the user is assuming the role of programmer.
- (c) Data base environments permit sharing of data among multiple application software systems. In the absence of some form of restriction by the computer systems users can access each other's data and the traditional concept of division of duties and independent nominal and general ledgers is compromised.
- (d) The mere fact that someone has access to a terminal can permit access to all the features of the application and system software. As a result, physical access restriction to the computer room, policies regarding division of duties and physical separation of people and records are no longer adequate fraud and intentional error safeguards.

Analysis of the above four points suggests that the traditional distinction between users and data processing personnel has become blurred and that the traditional controls over data processing personnel may now also be required over users, and vice versa. Unless the computer is used to enforce controls such as division of duties and addresses the areas listed below, it is doubtful whether a medium to large business would be able to implement an adequate system of internal control. The areas that need to be addressed specifically are:

- (a) Program security as means of access to data files.
- (b) System software security as a means of implementing and/or bypassing computer security.
- (c) Data file security as "representing" the business's assets and records.

- (d) Access control as a means of preventing unauthorised access to computing capabilities, enforcing division of duties and maintaining independent records where necessary.

For purposes of this hypothesis it is assumed that the mechanisms are available. Details of implementation and evaluation of security falls outside the scope of this dissertation as it would require extensive assessment of the issues involved.

III SUMMARY

The hypothesis for interfacing application and integrity controls has been defined in terms of four objectives:

- (a) Completeness and accuracy over transient data.
- (b) Completeness and accuracy over stored data.
- (c) Validity of transient data and changes to stored data.
- (d) Safeguard against intentional errors and fraud.

In some cases it is possible to substitute integrity controls for application controls and as such a direct or one-to-one relationship exists. On the other hand, many areas do not facilitate such a direct relationship and the best interface is reliance on programmed procedures to provide the basis for control. The investigation and correction of errors and exceptions remains as an application control. A number of observations are of significance:-

- (a) The interface is defined at a control technique level in accordance with the postulate which states that the application and integrity controls are useful ways of classifying control techniques.
- (b) Effective control is always a balanced combination of application and integrity controls; both specified at the application software level.

- (c) It is theoretically possible to have an environment which is fully controlled by users provided that all programmed procedures used as a basis for control are reperformed by the user. In the absence of integrity controls a user is not entitled to simply accept the results of computer processing.
- (d) Contemporary technology has a significant impact on traditional safeguards against fraud and intentional errors. The reason is the blurred distinction between the user component and data processing component of an on-line system.
- (e) Generic control models can be specified but it would be generic at the control objective level only. It appears, based on research for purposes of this dissertation, that a more generic interface is not possible based on current computer technology and understanding of auditing principles.

VALIDITY OF THE CONTROL MODEL AND THE INTERFACE HYPOTHESIS

To determine the validity of the control model and the hypothesis for interfacing application and integrity controls it is essential to use the run-time environment of a large modern computer system as a reference. This facilitates reference to a more realistic data path specification and enables proving of the hypothesis. The following headings have been used:

- I. COMPUTER RUN TIME ENVIRONMENT.
- II. DATA PATH, TASK INTEGRITY AND DATA INTEGRITY.
- III. PROOF OF HYPOTHETICAL CONTROL MODEL.
- IV. PROOF OF INTERFACE HYPOTHESIS.

I. COMPUTER RUN TIME ENVIRONMENT

As a basis for assembling a run time structure of a computer system the publication by H. Lorin and H.M. Deitel (9) has been used for the following reasons:

- (a) It is a recent publication.
- (b) Specific reference are made to system software on which much of the terminology in this dissertation is based.
- (c) It is authoritative and representative of a substantial portion of modern technology in view of its coverage of International Business Machine's technology.

It is important to note that the auditing perspective of system software is not based on the structural components but on the functional aspects which are evident during the run time phase. Most, if not all modern computers are based on a CPU (Central Processing Unit) including main memory, and sometimes additional slave processors which are used to perform specialised functions such as input and output. This structure implies that the computer can physically only perform one operation at a time when using the CPU. Although slave processors are used, the activation and final control over say input and output is still by system software running on the CPU - H. Lorin, H.M. Deitel (9/5,33,172). A number of points which impact on controls arise:

- a) In order to share the CPU the various system and application software required at run time is physically rolled in and out of the CPU at run time. Task integrity is therefore essential to ensure that data is not corrupted while an application program is rolled in or rolled out of the CPU at run time.
- b) Failure of any systems software component can affect task integrity and unless this is communicated to application program or a human operator the problem may not be detected. As a result data integrity may be compromised, erroneous data stored on files or erroneous output produced. An interface between a program and the system software services utilised is required. Quite often a basic interface is provided by the control language (Job Control Language (JCL)) H. Lorin, H.M. Deitel (9/45) which defines the application software to the system software.
- c) In other instances the application program is informed by the system software whether a transaction has been processed properly and that no error conditions were present. Unless the interface is properly programmed it can have the same affect as (b) above.

- d) The manner in which system software is set-up and defined to the computer affects the way in which the computer "behaves". A process called a SYSGEN (System Generation) H. Lorin, H.M. Deitel (9/195, 196) is used for this purpose. Both task and data integrity can be affected by selection wrong or improper options at SYSGEN time. This is covered in the hypothesis under the title "System Software Interface" as an interface is only possible once the underlying options have been selected.

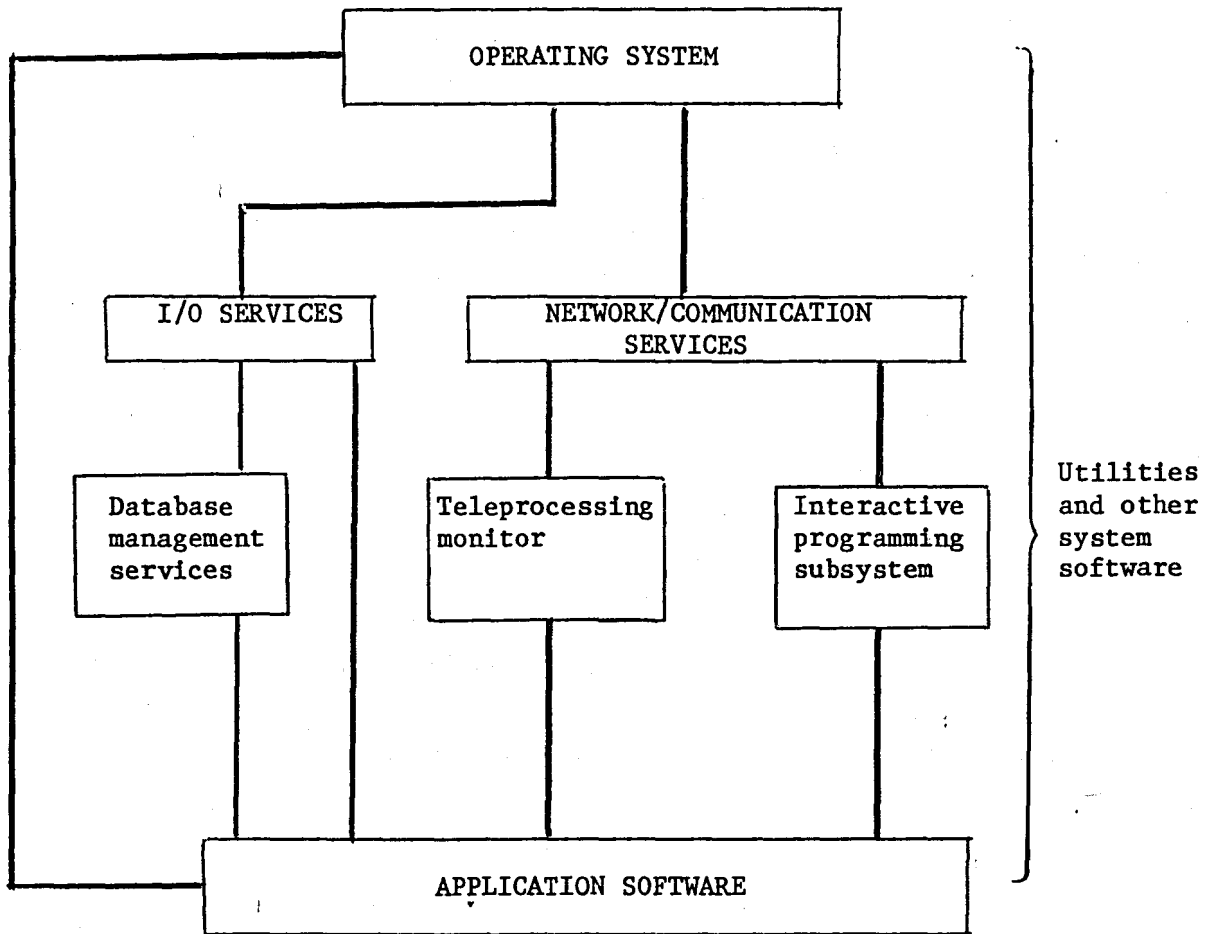
Run Time Environment

Most modern computer systems do not consist only of an operating system as far as system software is concerned. Using the common features contained in the publication used for this research, a modern computer system would typically include:

<u>Component</u>	<u>Reference in H. Lorin, H.M. Deitel (9)</u>
Operating System	24 et seq
Teleprocessing Monitor (Specialised Monitors)	92 et seq
Network/Communication Services	94 et seq
Input/Output Services	143 et seq
Compilers and Linkage Editors	191 et seq
Database Management Services	211 et seq
Interactive Programming Subsystem	214 et seq

Other features usually present are various utility programs, library packages which are used to manage programs stored on the machine, tape management systems and a number of systems which are used to manage the performance of the system.

The relationship of the various systems components at run time can be represented by the following hierarchy:



It is clear that there is a complex interaction of software in a computer system and the points made previously in this section indicate the need for concepts such as data paths and task integrity. Of significance is the incomplexity of the application program itself as many of the sophisticated functions are performed by system software including the roll-in roll-out or swapping required as only one CPU is normally available. The functions of each component is summarized below. Note that a typical configuration is described and the options may vary between systems.

Functions of System Software Components

Operating System

- . Managing CPU activities
- . Managing the memory of the computer
- . Managing the devices attached to the computer.
- . Managing the program initiation and interprogram communication
- . Managing data

Input/Output Services

- . Assists with the handling of different file types
- . Provides input/output services to application and other software

Network/Communication Services

- . Handling all areas of telecommunication services required by a computer system

Database Management Services

- . Handling the management of complex data structures
- . Providing sophisticated input/output facilities for application software
- . Providing extensive data integrity support services

Teleprocessing Monitor

- . Provides a high level of interface between network/communication services and application software
- . Manages transactions when input into the systems and assists with the scheduling of the appropriate programs
- . Assists with task and data integrity

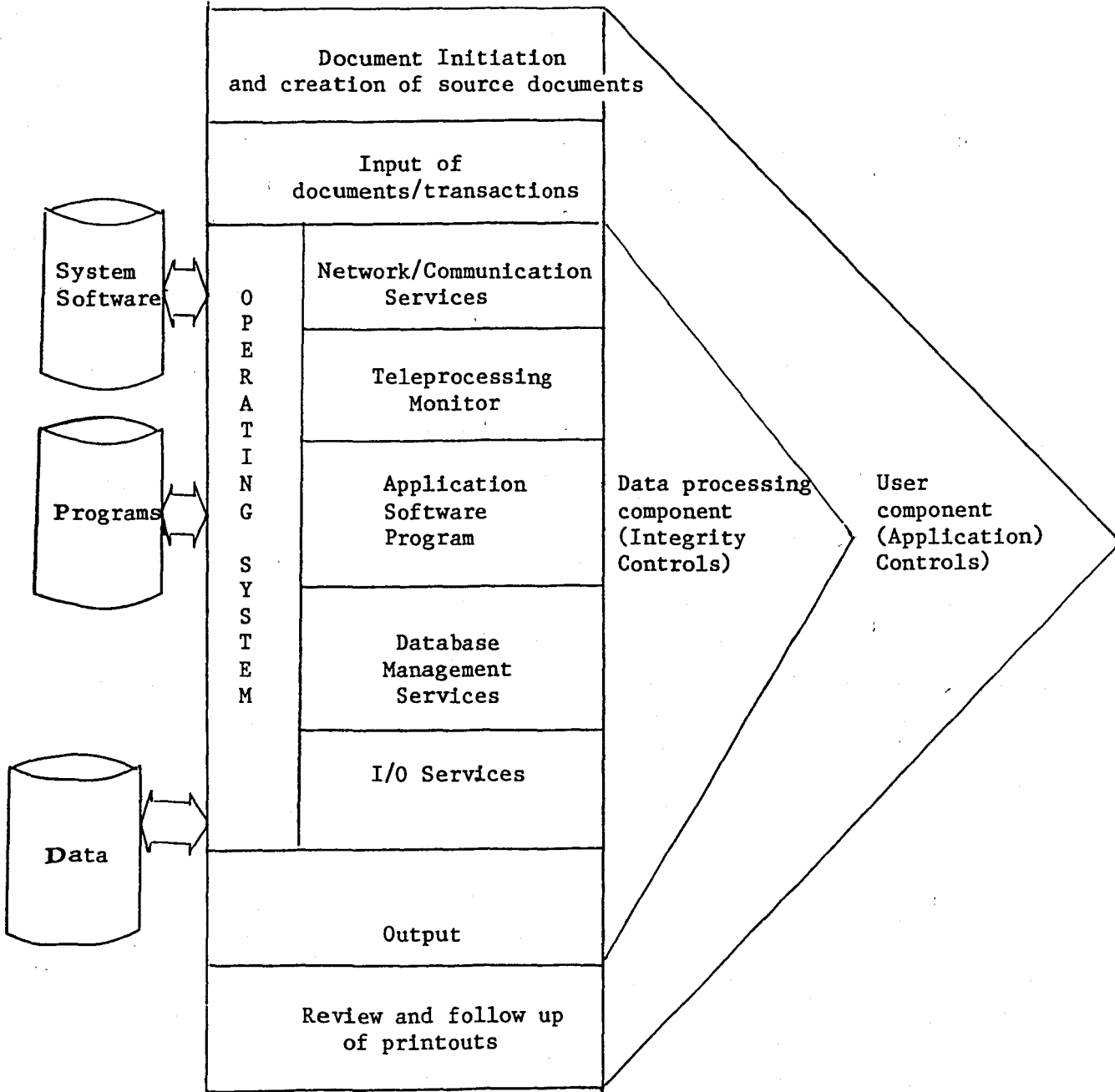
Interactive Programming Subsystem

- . Provides for on-line development and maintenance of application and system software
- . Allows for scheduling of jobs which run in batch mode
- . Permits on-line execution of many utilities which assist with proper performance of data processing activities
- . Contains a general editor and file management component
- . Provides a mechanism for distributing computational power and storage space

II DATA PATH, TASK INTEGRITY

Data Path

Using the concepts which have been defined in part I above, a typical data path of an on-line system can be represented as follows:



The data path concept which has been defined as one component of the control model comlies with system software theory and it is possible to conclude that the concept is valid as the path exists in a typical computer system, and accurate as it defines the relationship between system software components that are used in a computer system.

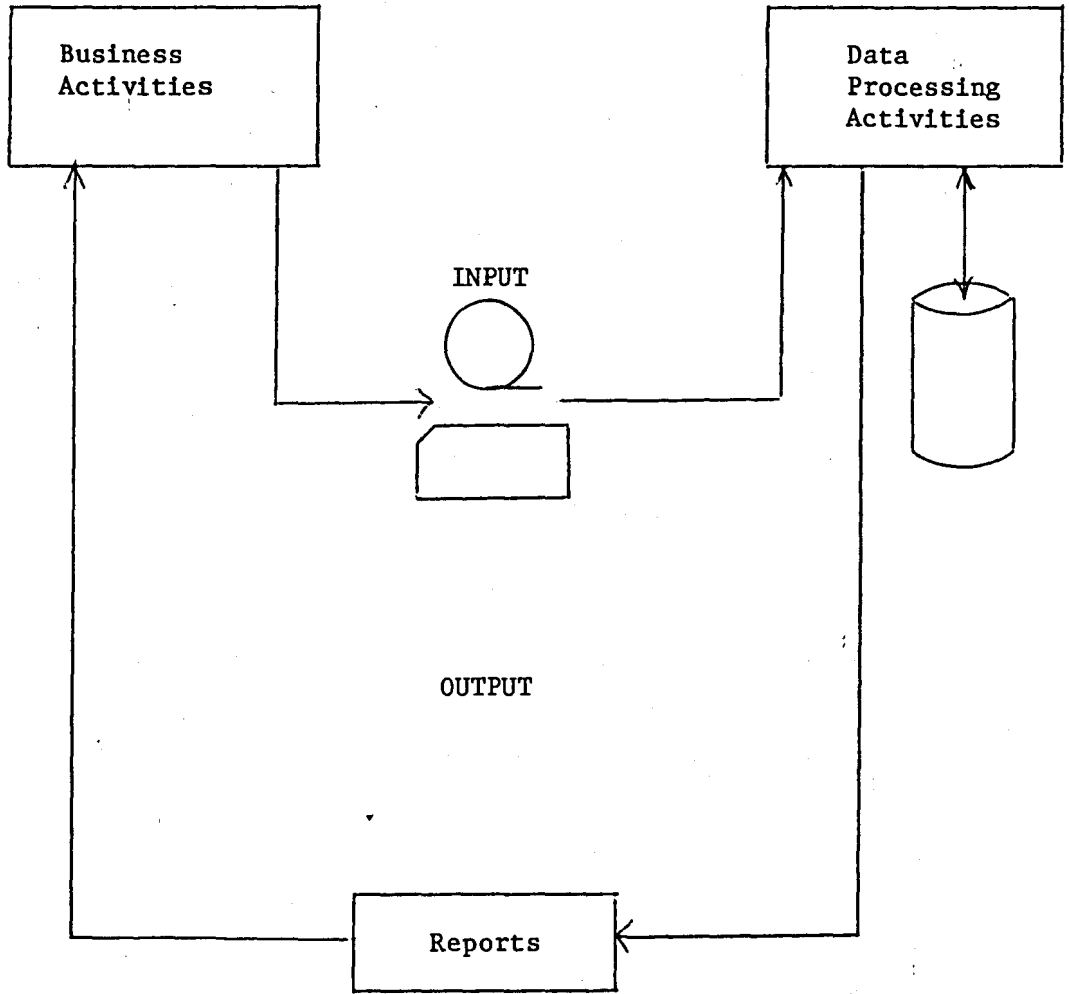
Task Integrity


Roll-in roll-out or swapping takes place within a computer as a result of having only one CPU and having seperate dedicated processors running under the control of the CPU using the operating system as a vehicle. Any accidental disruption of this process such as incorrect operator activities could, as explained above, lead to the data path component not running properly. It is logical that any control model needs to incorporate task integrity in its structure. The hypothesis has included this concept in all computer based control component as a seperate item because of its significance.


III PROOF OF HYPOTHETICAL CONTROL MODEL

A. Background

In the 1960-1970 period most computer systems were batch orientated ie. data was first captured and processed at a later stage, and divorced from the organisations business activities. Data was transported physically to and from the computer using media such as punch cards, magnetic tapes, paper tape for input and large volumes of printouts for output. This type of system can be illustrated as follows:



 = Punch Cards

 = Magnetic/Paper Tape

Under the circumstances the users were often responsible to ensure that all control objectives were achieved (viz completeness, accuracy, authorisation and maintenance). In most cases the machine was simply used to perform routine functions and produce a complete hard copy of the audit trail in order that inquiry functions and checking could be performed by the users. The data processing department was typically responsible for:

- i) Implementing and maintaining application software.
- ii) Security - Usually physical security as access to computer resources was via a physical medium or the computer console.
- iii) Computer Operations - All jobs and programs, including inquiries, compilations and charges to the operating system were run by the computer operator.
- iv) System software.

The above type of systems gave rise to the auditors first involvement with computer systems and a number of control issues arose from this type of system:

- i) There was a distinct separation between the various user departments and the data processing function. This separation both physical and functional in terms of responsibility. For example, there is no question about who performs the programming or the computer operations function.

- ii) As access to the computer resources was via some physical media or the operator's console which is located in the computer room , it was easy to implement security as it simply meant controlling physical access. Physical access controls cover access to the computer room and the ability to gain access to punch cards, paper tapes etc. By introducing procedures for authorising input prior to processing or authorising specific jobs there were few problems with security. Unauthorised access to data was also protected this way.

- iii) The computer operator assumed responsibility for every activity carried out by the computer as all the resources are under his control. Typically that persons responsibility included:
 - a) Getting a job in the computers job queue by placing the punch cards for the job in the card reader.

 - b) Starting a job by entering an appropriate command from the console.

 - c) Monitoring the correct disks or tapes on the relevant devices.

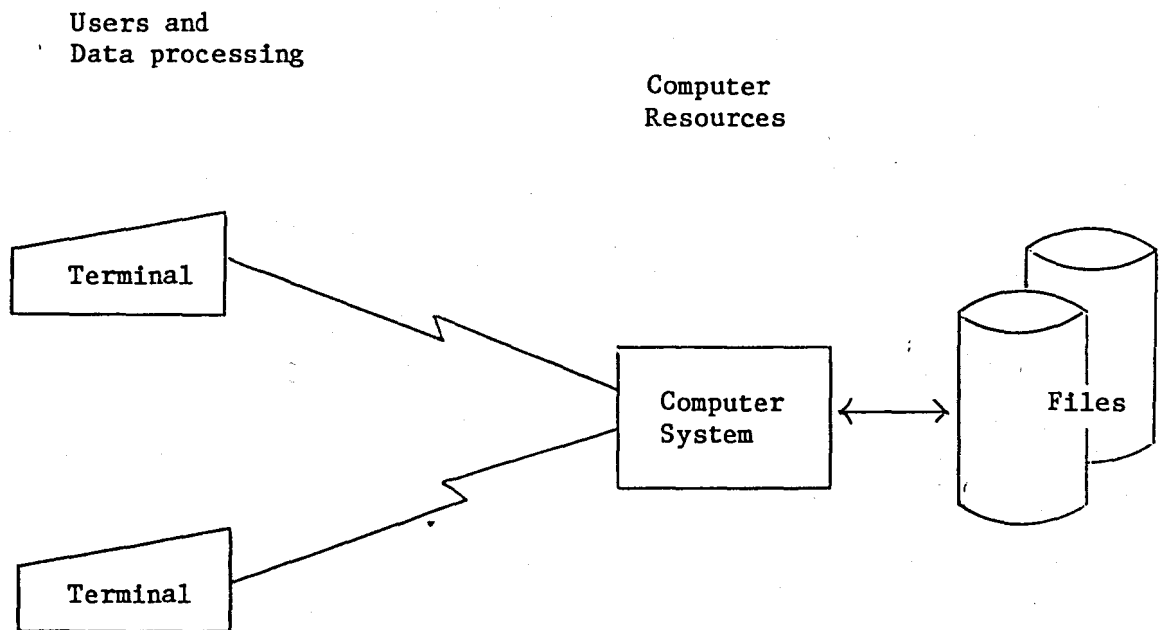
 - d) Handling certain error conditions which are reported on the operator console such as when unknown data files are requested by the program.

It is important to note that these functions covered all aspects of computer operations.

- iv) Evaluation of controls in such an environment allowed the auditor to evaluate integrity controls as a separate issue and on a general basis as all jobs were subject to the same controls. It was this environment which probably gave rise to the terms general or data center controls which are still used today.

B. A Modern Computer installation

Details in Part I of this section do not facilitate a simplistic view of a computer system and therefore a simple control model. Once an on-line system is introduced many of the traditional control considerations become obsolete. Compare the following diagram of a modern computer system with that of a batch system.



In this type of system the user typically involves programs from a terminal or the programmers submit program compilations without the computer operator being aware of it. The user sitting in front of a terminal controls his own processing and is sometimes even permitted to write his own application programs. It is clear that this gives rise to a new spectrum of control considerations. The more significant ones are:

- 1) The distinction between the functions of users and data processing has become blurred as many of the controls traditionally performed by data processing is migrated to the users. The best example is capturing and processing of transactions which is now usually done by a user using a terminal.

ii) Potentially all computer facilities are available to every terminal user. This means physical security is no longer adequate to provide computer security as the mere access to a terminal means access to all computing facilities. Security has now become a complex issue as it is necessary for the computer systems to:

- * Ensure that data processing staff do not have access to financial and other live systems.
- * Distinguish between users in order that the concept of division of duties be preserved. One does not for example want everyone having access to the payroll or creditors systems.

iii) As the quality and complexity of system software increased many of the traditional manual functions have become automated. Examples of such system software are teleprocessing monitors and database management systems. Application programs often rely on many of these control functions and as such the area of system development and maintenance becomes more complex as a result of interfacing with the system software.

C. Proof of Control Model

To prove that the control model which has been defined in the hypothesis can accommodate a modern computer system more effectively can be regarded as an evaluation of three alternatives based on the considerations discussed above.

a) Alternative 1

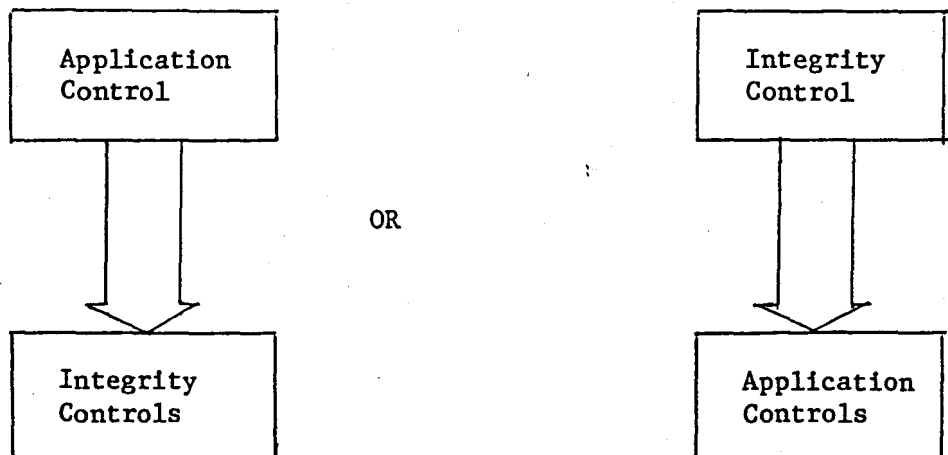
Application Controls

Integrity Controls

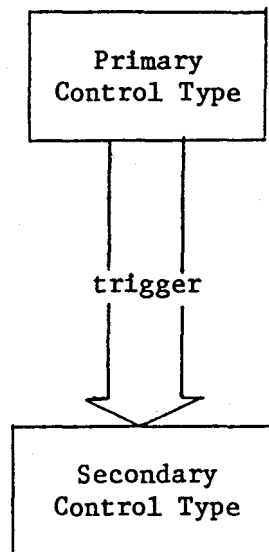
This model views application and integrity controls as two separate issues with no substituting or complementing of control types. A model such as this cannot accommodate an on-line systems as it does not have a mechanism to relate the system software control function, the application and the application controls. Based on the previous sections it is obvious that:

- i) Consideration of one control component in isolation results in the migration of control from users to system software or data processing, or vice versa, remaining undetected which in turn may conceal significant control exposures.
- ii) Division of duties is enforced by computer security in an on-line system. By ignoring this when evaluating application controls it is impossible to determine which users are performing various functions in the computer system.
- iii) Acknowledging that many modern computer systems are complex and cannot be controlled adequately by users it becomes essential that the automated procedures on which control is based be considered as an integrated part of the system. To achieve this a control model would need to provide an interface at an application level.

b) Alternative 2



Essentially this model is based on a structure of a primary control type providing triggers into a secondary control type viz:



Individual control objectives such as completeness, accuracy and validity are considered under the primary control type and only insofar as reliance on a second control type needs to compensate for deficiencies in the primary control type. It also assumes that only the control objectives within the primary control type are significant as this is the only way a trigger mechanism or printer to the secondary control type can exist. There is no other entry point into the secondary control type. This model therefore takes care of compensating controls but cannot handle substitution of controls. The hypothesis provides the outlines of the proposed compensation and substitution of controls.

Having established the two problems with this model i.e. inability to consider control objectives in the secondary control type and inability to substitute controls, the necessity of these features needs to be examined. Assume that the auditor is evaluating application controls as a primary control type and that the specifics concern stored data. Assume that the user control is a spot check during the year of the file's contents. This control would be identified as being the primary control. There is however, still a risk that erroneous items may remain undetected or introduced after checking by the user. The reason for this is the timing, (the point in time) and consistency of the check. By consistency we mean that the user may not perform his functions with the same consistency over a period of time.

On the other hand modern computer systems contain sophisticated mechanisms, to minimise the corruption of data. Lorin and Deitel (9/7) describe examples of the interrupt system which takes care of processor and other failures. In addition data base management systems contain utility programs to ensure that the file structures are not corrupted. The nature of computers permit them to perform programmed procedures more consistently than users perform functions.

It may therefore be desirable to substitute the user control described above with the integrity control mentioned. By first directing the auditor to an application control, the auditor has not considered the substitute which may be more effective, efficient and more appropriate to rely on for audit purposes. Another consideration is the degree of difficulty encountered in practice where businesses rely on detective controls to detect error and fraud. The characteristic of such controls is that they result in discovery of problems after they have occurred. Whilst it may be useful to state that the user will detect the fact that transaction or data files have been deleted the subsequent corrective measures may involve substantial administrative effort.

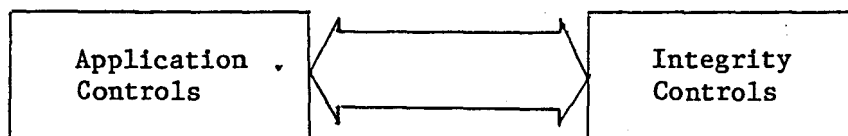
On the other hand integrity controls provide the preventative controls to reduce the risk of the problem occurring.

Obviously the latter is the more reliable and effective alternative.

The advantages of this alternative, unlike alternative 1, is that an interface between application and integrity control does exist albeit at a simplistic level. Its shortcomings does limit its application and it does not permit balancing application and integrity controls in the most effective way. The interface does not always define the situation in such a way that the total system is considered.

c) Alternative 3

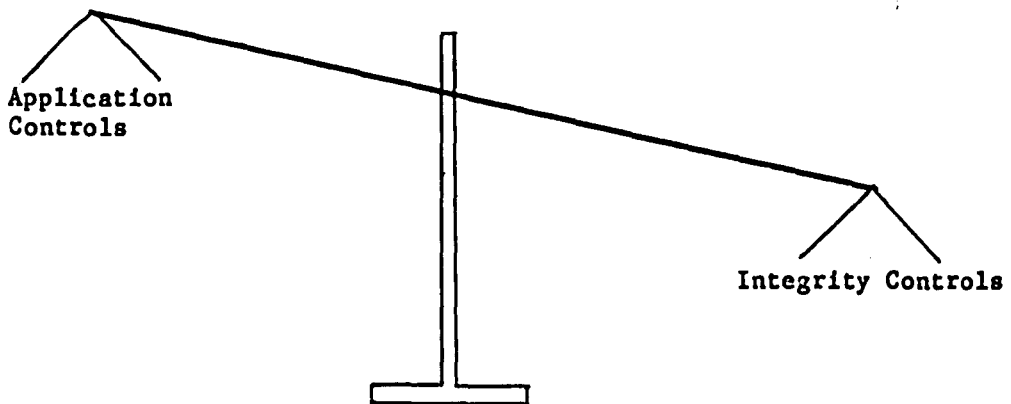
The hypothetical control model proposes a model with application and integrity controls at peer levels viz.



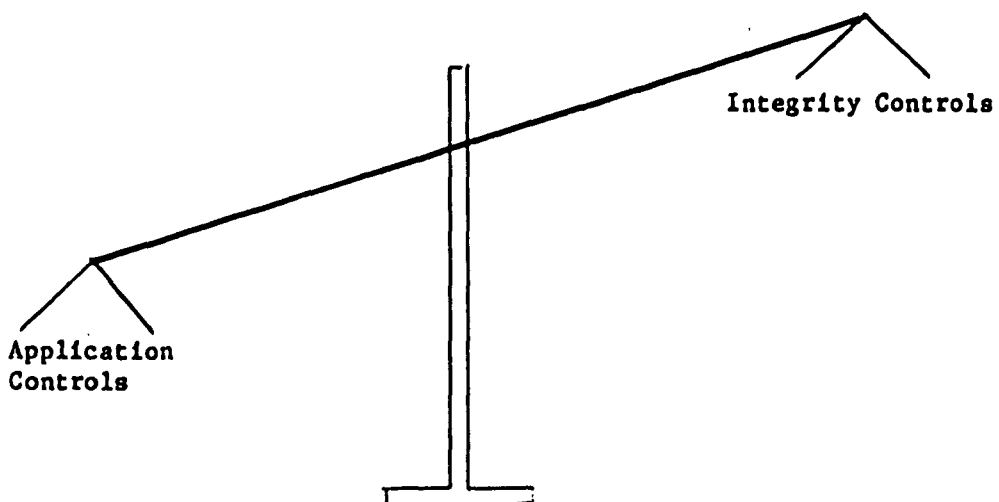
It permits substitution of control types at peer level as well as compensation of each other. Essentially it is possible to start with any control type, evaluate a specific objective and determine where the control is in place. The auditor can even start with a specific integrity control and determine whether it is compensated by an application control or assured by one (this would be substitution). As computers become more complex and system software more powerful there may be a gradual shift of control to integrity controls. By having a "peer" model of control types this shift can be easily accommodated even to the extent that integrity controls becomes the primary control type as discussed in the previous section. A number of other observations can be made about this model.

- a) Although it is becoming impracticable it is possible to have a pure user controlled system. Under these circumstances everything performed by the computer is checked in one way or another by the user. This model takes care of such a system by ignoring the integrity control side.
- b) In a smaller business system where there is often an absence of sophisticated system software and therefore some system software based control features. The control model views the total system and by establishing a control bias towards user controls it is possible to attain the required degree of control. These issues can be illustrated as follows:

Sophisticated Computer System



Unsophisticated Computer System



The key advantage of this model is that by having the control types at a peer level controls can be evaluated, or designed, by considering both the user and data processing component objectively and efficiently with the process of substitution or compensation.

Conclusion

The most general model for interfacing application and integrity controls is the peer model which describes the interface by defining the two control types at a peer level. One of the most obvious advantages is that the data processing component of a system is not ranked less important and of secondary interest to the auditor. It provides an objective way to describe the interface between two control types which are quite different in nature. Any other model can be derived from the peer model by assuming secondary importance to it. We therefore conclude that the hypothetical model described is the most ideal and general model for interfacing application and integrity controls.

IV PROOF OF INTERFACE HYPOTHESIS

In the previous section the generic model for interfacing application and integrity controls was confirmed. Having established that the best solution is the peer model we can proceed to prove the detailed interface hypothesis i.e. the components of the model described in the previous section. To achieve this we need to reconsider the nature and extent of integrity controls.

a) Nature of Integrity Controls

Our definition of integrity controls state they are "... those manual, system software based controls which are exercised or directed by the data processing over transient and stored data". It is a generally accepted auditing principle that the data processing department should not be responsible for performing application controls but are there to ensure that systems are properly developed and maintained, secured, used and that the system software used is adequately maintained. This statement is evident from the literature survey as all of these issues were addressed in one way or another. Should one examine the above areas it becomes evident that controls over those functions are necessary to process data accurately and ensure that accuracy anywhere in the data path ie. while transient and thereafter when stored. Translating this into the definitions which have been established previously, the objectives of integrity controls are to ensure task and data integrity and that programmed procedures for processing data are in place. The role of integrity controls as a safeguard against fraud eg. by enforcing division of duties using computer security, has been ignored for purposes of this dissertation. Because the definition of integrity controls forms the basis for proving the hypothesis it is essential to confirm it with the literature used in this dissertation. The following table presents the summary of the literature study.

Reference	Component	Application Controls	Integrity Controls
Davis G.B. (1)	General Systems Controls		X
	Specific Application Controls		
	- Input and Output Controls	X	X
	- Processing Controls	X	X
	- Audit Trails	Not a control as such	
Jenkins B & Pinkney A (2)	Application Controls	X	
	Integrity Controls		X
The IIA (3)	Application Systems Controls		
	- Transaction Origination	X	
	- Data Processing Transaction Entry	X	X
	- Data Communications		X
	- Computer Processing	X	X
	- Data Storage and Retrieval		X
	- Output Processing	X	X
	General Controls		X
The CICA (8)	Pre-installation Controls		X
	Organisational Controls	X	X
	Development Controls		X
	Operations Controls		X
	Processing Controls	X	X
	Documentation Controls		X

The nature of the items described in the table as integrity controls support this viewpoint. Another way to prove this is by examination of a typical business environment.

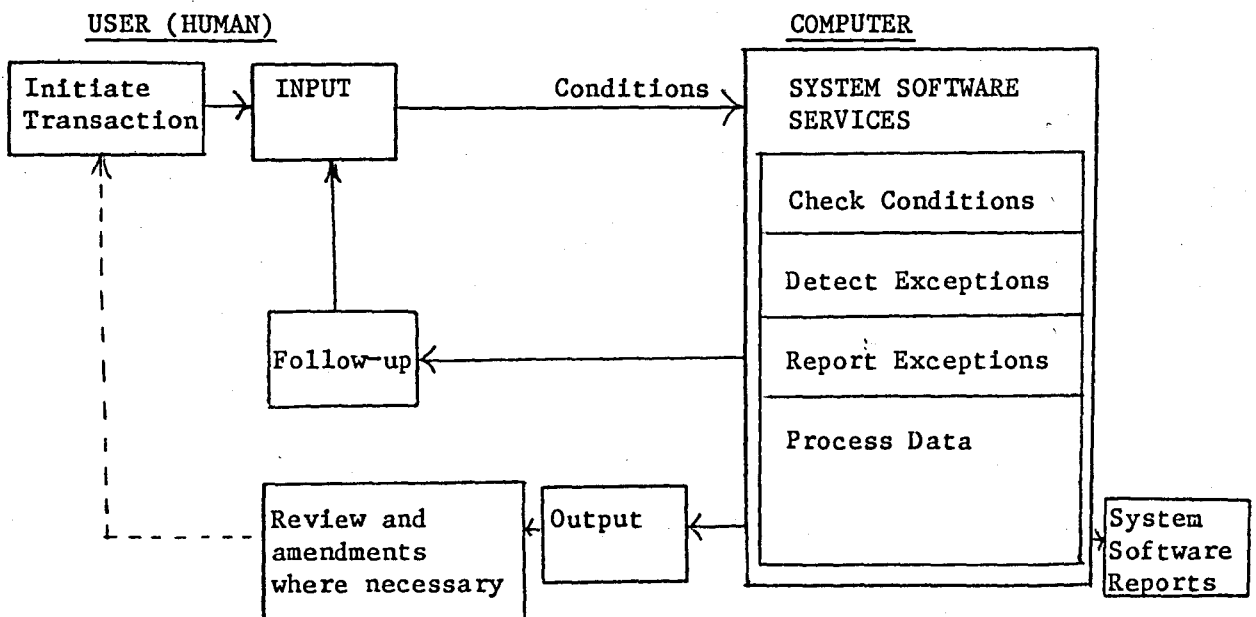
- (i) Only certain users are authorised to initiate and process business transactions. Internal control is also geared to ensure that no unauthorised amendments are made to transactions once they have passed through the checking and approval procedures. In a manual system this is normally achieved by instituting division of duties where checks by other persons ensure "task" and "data" integrity. Where the system is automated many of these procedures are incorporated into the software
- (ii) One of the reasons for automating procedures is the high degree of consistency with which the computer would apply them. It is however necessary to ensure that they remain unchanged and that while data is being processed, and subsequently stored, no errors are introduced. To a business it means that reliance is placed on the computer system and information obtained from it is considered accurate and used for conducting business.
- (iii) Computers are more consistent because the hardware and software provides the facilities to assure task and data integrity provided the applications have been properly implemented and maintained. This in fact provides the basis for establishing controls.
- (iv) Although many other factors can also be considered the above is sufficient to illustrate the nature of integrity controls. Obviously they are different to application controls which are directed towards the user component of a system. The two control types do however have certain common overall objectives viz. prevention and/or detection of errors and fraud in the broader sense. To determine whether the hypothetical interface is accurate it is, however, necessary to look at the differences as well.

b) Interfacing Application and Integrity Controls

It has been established previously that control objectives can be classified as:

- i) Completeness and accuracy over transient data
- ii) Completeness and accuracy over stored data
- iii) Validity of transient data and changes to stored data
- iv) Safeguard against intentional errors and fraud

A definition of control which includes the user (human) input and correction phase has also been explained in the computer control hypothesis section. The following diagram was used. (It has been expanded to incorporate processing activities):



Examining the control objectives and the above representation a number of rudimentary facts are evident which, although impossible to prove formally, are intuitively obvious:

- (i) A computer can be used to perform some of the routine procedures which people performed in a manual system.
- (ii) Routine functions include initiating certain transactions (eg. interest), checking data for exceptions, reporting exceptions, processing accurate data and providing output.
- (iii) Computers cannot at this point in time follow up exceptions, review output and initiate other transactions in response to unusual items in the output. Note that the data in the output is considered accurate by the computer but it may not be correct in the business sense of the word.
- (iv) Computers are unable to initiate transactions which require translation into another format eg. an order from a client needs to be translated to identify the stock code or the specific item as held on a stock master file. By way of a general statement it can be said that a modern computer still requires a substantial human interface.

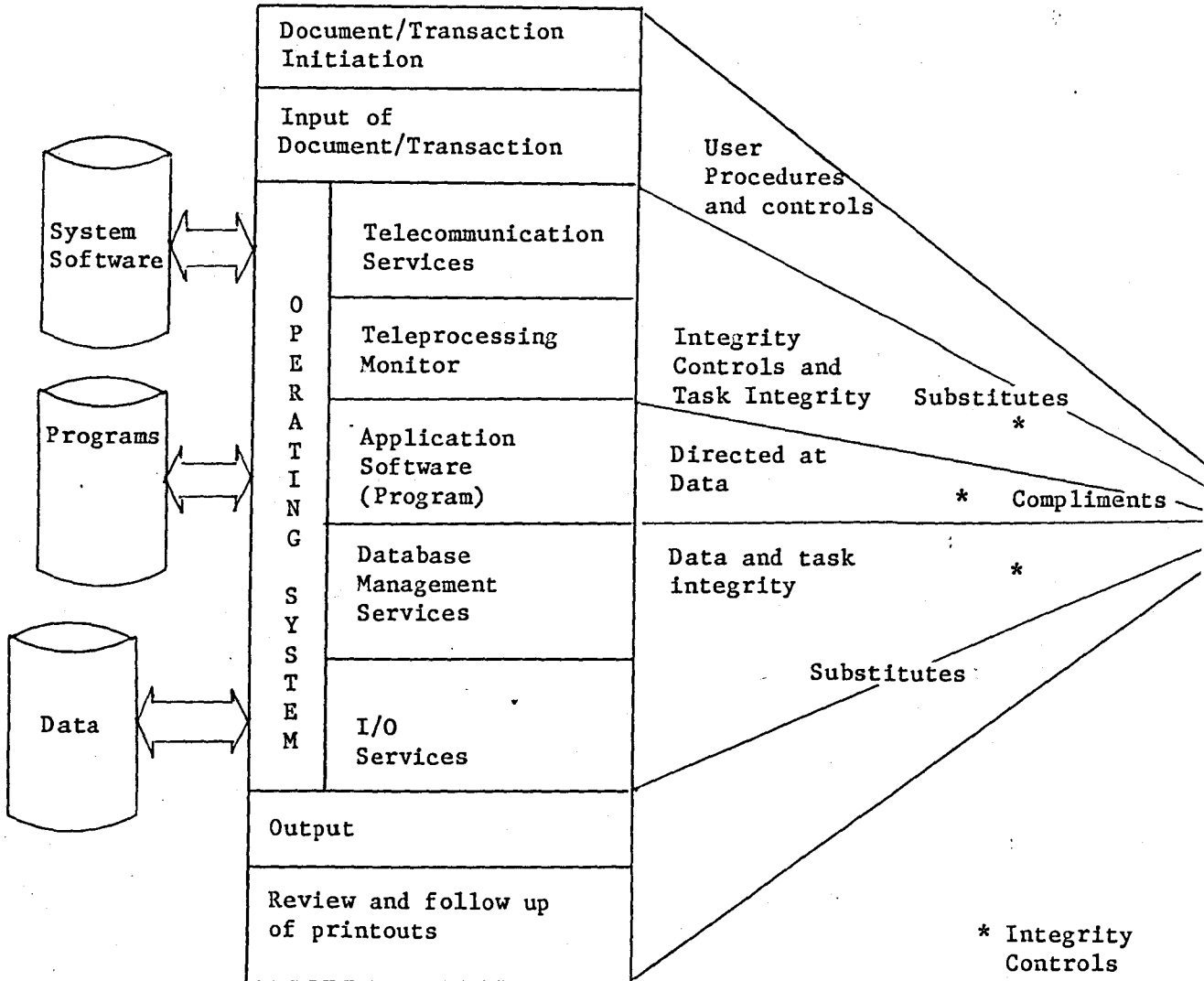
Based on these facts a pattern emerges:

- (i) Computers cannot perform those parts of controls which require non-routine procedures to function properly. At best the routine procedures that need to be performed to enable the non-routine procedures to be carried out can be incorporated into a computer system.
- (ii) Where routine procedures are used to ensure task and data integrity they can be incorporated into the computer system.

(iii) In the event of procedures being carried out by a computer the term programmed procedures are used as human or user procedures. User controls assume that user procedures are accurate by re-checking the work, division of duties and supervision. Integrity controls assure that programmed procedures continue to operate properly.

It is impossible to make certain conclusions which constitutes the conceptual foundation for proving the hypothesis. The first deals with the substitution between the control types. Where a procedure is performed to ensure task and data integrity it is irrelevant whether an application or integrity control is used as they can be substituted directly. The nature of the exception reporting and follow-up are different but the result is the same. On the other hand where procedures are directed to prevent or detect specific errors in data while transient or stored the only part that can be automated are the routine procedures on which a review or follow-up of exceptions is based. System software described in part I of this section does not operate on data itself and at best can report the inconsistent functioning of the environment in which a specific application exists ie. task and data integrity.

Should specific procedures be necessary to operate in data an application program is required and integrity controls could ensure that it is properly implemented, maintained and executed. At this level substitution of control types is not possible but integrity controls complement the application controls by taking care of the routine procedures, ensuring the adequacy of the programmed procedures, task and data integrity. Data path diagrams discussed in part II of this section confirm this.



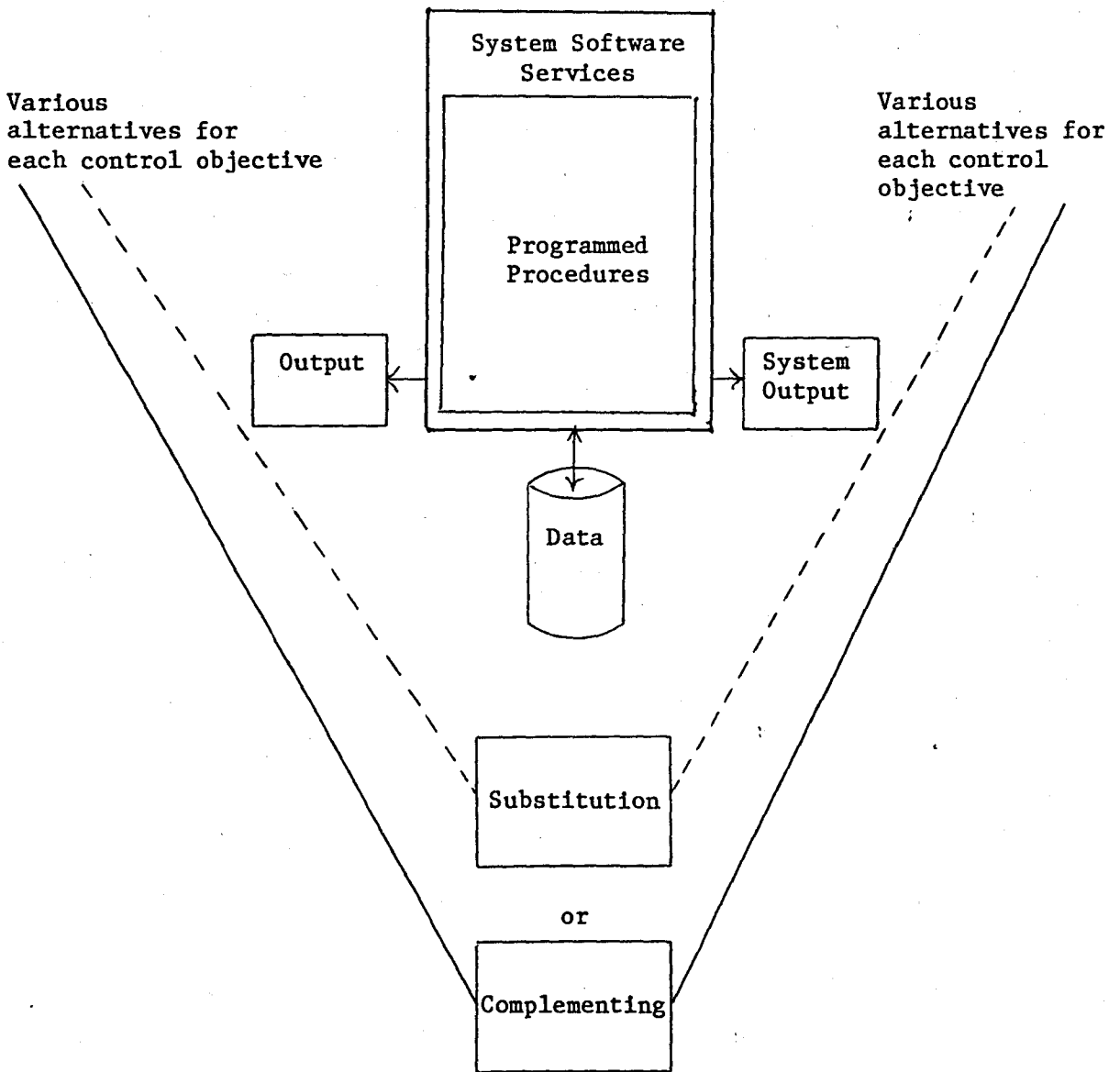
DATA PATH DIAGRAM

Since the operating environment of applications may vary eg. some may not involve on-line or data base components it is not possible to assess the integrity controls on a general basis. Part I of this section highlights some of the issues when interfacing the application program with other sytem software. The issues are clearly not generic and evaluation on an application basis is necessary. It is possible to represent a generic model to evaluate controls on an application basis by simplifying the data path program.

Application Controls

Computer

Integrity Controls



where applicable

The derived model complies with the reasoning and background provided in parts I to III of this section. Not only does the model cater for modern computer systems but it provides the auditor with the reasons for evaluating integrity controls. The details hypothesis for interfacing application and integrity controls was presented on this basis. Reasons for complementing certain controls and substituting others are also presented there while the additional considerations have been discussed in this section.

c) Conclusion

A control model which facilitates the interfacing between application and integrity controls has been derived and proved in relation to modern computer systems and general audit control theory. Of significance is the role of integrity controls in the control of computer systems and its relative importance in some areas and greater importance in others.

BIBLIOGRAPHY

1. Davis, G.B. Auditing & EDP, 1978 The American Institute of Certified Public Accountants, Inc.
2. Jenkins, B. and Pinkney, A., An Audit Approach to Computers, 1975, The Institute of Chartered Accountants in England and Wales.
3. Stanford Research Institute for the Institute of Internal Auditors, Systems Auditability & Control - Control Practices, 1977, The Institute of Internal Auditors.
4. Stanford Research Institute for the Institute of Internal Auditors, Systems Auditability & Control - Audit Practices, 1977, The Institute of Internal Auditors.
5. The American Institute of Certified Public Accountants - Computer Services Guidelines, Management, Control and Audit of Advanced EDP Systems, 1977, American Institute of Certified Public Accountants, Inc.
6. The American Institute of Certified Public Accountants - Computer Services Guidelines, Controls over Using and Changing Computer Programs, 1979, American Institute of Certified Public Accountants, Inc.
7. The Canadian Institute of Chartered Accountants - Computer Audit Guidelines, 1975, The Canadian Institute of Chartered Accountants.
8. The Canadian Institute of Chartered Accountants - Computer Control Guidelines, 1973, The Canadian Institute of Chartered Accountants.
9. H. Lorin, H.M. Deitel - Operating Systems, 1981 Addison-Wesley Publishing Company Inc.
10. The South African Institute of Chartered Accountants, Statement AU230 - Internal Control.