AN AUDIT APPROACH TO RISKS AND CONTROLS IN THE VIRTUAL ENTERPRISE

By

CHARL VAN REENEN BRITZ

SHORT DISSERTATION

Submitted in partial fulfilment of the requirements for the degree

MASTER OF COMMERCE

In

COMPUTER AUDITING

In the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

At the

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF. A. DU TOIT

Johannesburg, November 1999

DECLARATION

I declare that this short dissertation hereby submitted to the Rand Afrikaans University for the degree of Master of Commerce, is my own, unaided work, except to the extent acknowledged in the text. It has not been previously submitted for any degree or examination to this or any other university.

Charl Van Reenen Britz

CONTENTS

OPSOMMING

'N OUDITBENADERING TOT RISIKO'S EN KONTROLES IN DIE VIRTUELE ONDERNEMING

Deur

Charl Van Reenen Britz

Opsomming van die skripsie ingedien

Vir die graad

Magister Commercii

In

Rekenaarouditering

Aan die

Fakulteit Ekonomiese en Bestuurswetenskappe

Aan die

Randse Afrikaanse Universiteit

Studieleier: Prof. A. Du Toit

Johannesburg
November 1999

'N OUDITBENADERING TOT RISIKO'S EN KONTROLES IN DIE VIRTUELE ONDERNEMING

Die doel van hierdie opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing weer te gee. Hierdie opsomming bestaan uit die volgende:

1. **Probleemomskrywing en doel van hierdie navorsing**
2. **Navorsingsmetodiek**
3. **Omvangsbeperkings en uitsluitings**
4. **Resultate**
5. **Gevolgtrekking**

1. PROBLEEMOMSKRYWING EN DOEL VAN HIERDIE NAVORSING

Volgens Grimshaw & Kwok (1998:45), het die samevoeging van rekenaarnetwerke en telekommunikasietegnologie dit vir groepe maatskappye moontlik gemaak om hul verpreide bevoegdhede te kombineer in 'n enkele virtuele onderneming en mededingende voordele in die proses te behaal. Hoe beïnvloed hierdie verwikkelinge die ouditeur se beplande ouditstrategie? Een van die faktore wat die ouditstrategie beïnvloed is die algehele beheeromgewing van die besigheid (Jenkins, Cooke & Quest, 1992:18).

Die doelwitte van hierdie skripsie is die volgende:

- Om die risiko's vanuit 'n ouditoogpunt te bepaal wat met die virtuele onderneming geassosieer word; en

- Om die kontroles te identifiseer wat die bestuur van die ouditeur se kliënt kan implementeer om die risiko's die hoof te bied.

2. NAVORSINGSMETODIEK

Twee afsonderlike literatuurstudies is onderneem om die doelwitte van die skripsie te bereik, naamlik:

- Die eerste literatuurstudie was om die konsep en kenmerke van die virtuele onderneming te identifiseer, insluitend die gebruik van inligtingstegnologie in virtuele ondernemings.

- Die tweede literatuurstudie ondersoek die ouditrisiko's en kontroles in 'n rekenaaromgewing ten einde 'n kontroleraamwerk te ontwikkel.

Die inligting vanuit bogenoemde twee literatuurstudies sal gebruik word om 'n kontroleraamwerk vir die oudit van risiko's en kontroles vir die virtuele onderneming te ontwikkel.

3. OMVANGSBEPERKINGS EN UITSLUITINGS

Die skripsie konsentreer uitsluitlik op 'n ondersoek na die risiko's en gepaardgaande kontroles in 'n virtuele onderneming wat relevant is vir die ouditeur. Die volgende word spesifiek uitgesluit:

- Die sogenaamde televerkope of telebemarkings organisasies wat hul goedere en dienste oor die Internet verkoop; en

- Plastiekkaarte en die gedetailleerde kontroles onder elk van die hoof kategorieë rekenaarkontroles.

4. RESULTATE

Die ouditeur behoort die volgende in ag te neem wanneer 'n oudit op die risiko's en verwante kontroles in die virtuele onderneming gedoen word:

- Die gerekenariseerde omgewing van die kliënt, bestaande uit beide die algemene en applikasie (toepassings) kontroles deur gebruik te maak van die rekenaarkontrolemodel soos gereflekteer in figuur 3.4;

- Die Internet risiko's en verwante kontroles; en

- Die risiko's en verwante kontroles van EDR (Elektroniese Data Ruiling) en EFO (Elektroniese Fonds Oorplasing) indien van 'n Waarde Toevoegings Netwerk ("Value added network") gebruik gemaak word.

5. GEVOLGTREKKING

Voor die navorsing gedoen was, was kennis omtrent die virtuele onderneming en spesifiek die risiko's wat dit vir die ouditeur inhou, beperk gewees. Die navorsing het bygedra tot beter kennis van die risiko's van die virtuele onderneming asook die verwante kontroles wat die risiko's sal aanspreek.

Hierdie navorsing het die volgende areas geïdentifiseer vir verdere navorsing:

- Die risiko's en kontroles indien die virtuele onderneming 'n geïntegreerde applikasieprogram ("ERP-Enterprise Resource Planning") gebruik;

- Die risiko's en kontroles indien daar verskeie losstaande applikasieprogramme is wat gekoppel is met die hoof-finansiële applikasieprogram ; en

- Die uitwerking op die ouditbenadering indien die hele of slegs 'n gedeelte van die virtuele onderneming die ouditeur se kliënt is.

SYNOPSIS

AN AUDIT APPROACH TO RISKS AND CONTROLS IN THE VIRTUAL ENTERPRISE

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THIS RESEARCH

"The convergence of computer networking and telecommunication technologies is making it possible for groups of companies to co-ordinate geographically and institutionally distributed capabilities into a single virtual organisation and to achieve powerful competitive advantages in the process" (Grimshaw & Kwok, 1998:45). To what extent do these developments effect the auditor's approach in determining his audit strategy? According to Jenkins, Cooke and Quest (1992:18), one of the factors that effects the audit strategy is the overall control environment of the business.

The objectives of this short dissertation will be:

- to identify the risks from an audit perspective that are associated with the virtual enterprise; and

- to identify controls which the management of the auditor's client could implement to minimise these risks.

2. RESEARCH METHODOLOGY

Two separate literature surveys were conducted in order to meet the objectives of this short dissertation:

- The first literature survey identified the concept and attributes of the virtual enterprise, including the use of information technology in virtual organisations.

- The second literature survey discussed the audit risks and controls in a computer environment in order to develop a control model.

Using the information obtained as a result of these two literature surveys, a framework for auditing risks and controls in a virtual enterprise was developed.

3. SCOPE AND LIMITATIONS

This short dissertation has concentrated exclusively on the investigation of risks and the related controls which are relevant to the auditor in the virtual enterprise. Certain limitations have been necessary in order to remain focused, namely:

- The so-called teleshopping or telemarketing organisation is excluded from this short dissertation; and

- Plastic cards and the detail controls under each of the main category of computer controls are also excluded.

4. RESULTS

In summary, the auditor will need to consider the following when reviewing the risks and controls in the virtual enterprise:

- The CIS Environment of his/her client, consisting of both the CIS General and Application Controls using the Computer Control Model as depicted in Figure 3.4;

- The Internet Risks and the associated controls; and

- EDI and EFT Risks and the associated controls if a VAN is used.

5. CONCLUSION

Before the present research project, knowledge of the virtual enterprise environment - specifically concerning the risks involved and how these risks will effect the auditor - was limited and anecdotal. It is hoped that the present research, specifically with regard to the auditor, has contributed towards a better understanding of the risks and the controls that would minimise these risks.

This short dissertation has opened the following areas for further academic research:

- The risks and controls if an integrated enterprise resource planning (ERP) application is used for the virtual enterprise;
- The risks and controls if various different applications are used that interface to the main application in the virtual enterprise; and
- The effect on the audit approach if the whole virtual enterprise or only certain companies in the virtual enterprise constitute the auditor's client.

CHAPTER 1

INTRODUCTION

CONTENTS PAGE

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

"The convergence of computer networking and telecommunication technologies is making it possible for groups of companies to co-ordinate geographically and institutionally distributed capabilities into a single virtual organisation and to achieve powerful competitive advantages in the process. Collaborative applications such as computer-based conferencing, shared databases, shared applications, workflow management, project management, and video-conferencing can be used to support dispersed people to work together" (Grimshaw & Kwok, 1998:45).

Palmer (1998:73) also shares this view when he states that virtual organisations are established because of the "interest in sharing information, developing standards and reducing costs".

Goldman, Nagel & Preiss (1995:94) are of the opinion that the current interest in virtual organisation structures was created due to the emergence of agile competition. The rapid development of new products and the introduction of these into high-value-added markets, together with the unpredictable character of new market opportunities and the evolving customer demands, has made it impossible for any company to maintain world-class capabilities from the one end of the production chain to the other. Increasingly, companies can compete successfully only if they have identified their own world-class competencies and are prepare to integrate them with the complementary capabilities possessed by other companies (Goldman et al.,1995:95).

According to Goldman et al., (1995:95) a company with a virtual organisational structure "substitutes bytes for bricks" by integrating those resources and capabilities required for a particular product virtually. Leaving them in place physically but knitting them together electronically, the company reduces the need to erect facilities or to hire personnel dedicated to the new product.

The following business trends have given rise to the virtual organisation (Goldman et al., 1995:229):

- The development of a worldwide communication and transportation system enabling worldwide sourcing and selling that in turn has created increased global competition and borderless economies;

- The creation of products and services in arbitrary lot sizes which in turn has fostered a demand for shorter life cycle and faster time to market;

- The development of the information-handling capacity to treat customers as individuals and not as statistical averages which led to increased product customisation. This increase in product customisation requires extended core competencies as well as a convergence of technologies;

- An increased information-handling capability makes information technology a key role enabler of enhanced communications; and

- With more sophisticated stakeholders, customers (and others demanding all these capabilities and complexities in a shrinking window of opportunity) foster the development of and use of the virtual organisation to share the risk and rewards in development efforts in order to provide the ability to deliver on stakeholder expectations.

It is against this background that the auditor and especially the computer auditor will need to determine what effect his/her client's involvement in such a virtual organisation will have on his/her audit approach.

1.2 PROBLEM DESCRIPTION

"Boeing's 777 passenger plane was created by about 250 cross-functional teams, including members from supplier companies and airline customers, distributed over a number of locations. All were linked electronically and through use of common CAD software. For the first time, a commercial airliner was created and put into production on a virtually paperless basis, using computer modelling almost exclusively. This significantly reduced both the cost and the time of development. In addition, Boeing assembled the plane from components and subassemblies manufactured by an alliance of domestic and foreign manufacturers of competing aircraft and of suppliers to such manufacturers" (Goldman et al., 1995:138).

This example clearly demonstrates integration of information technology, design and manufacturing processes, remote cross-functional teaming and peer-level supplier and customer interactive relationships, all components in a virtual organisation.

Grimshaw and Kwok (1998:57/58) also provided a case study example of a virtual organisation:

" Sonicon is a graphic design company serving the record industry and computer games market. Its business activities include creative design, digital artwork and graphic reproduction. ... In order to improve communication between designers and clients, and the quality of design and artwork, Sonicon has implemented a programme in 1990, which includes the development of hardware and software technology that are compatible with its major clients and trains its people so that they can work in the new environment. This enables Sonicon to support *collaboration* with clients, for example Virgin and EMI, in international projects via an Integrated Services Digital Network (ISDN) link incorporating shared application tools such as Acrobat and Forecast. With the use of the ISDN technology, designers can send big colour files to the clients around the world... The new technology also allows designers, from different companies forming a project *alliance,* to work on the same project via the network at the same time".

This example illustrates the following attributes of a virtual organisation: Alliance for a common goal, underlying information and communication technologies, vertical integration, globalisation and collaboration (Grimshaw & Kwok, 1998:68).

The question that remains is, 'To what extent do these developments effect the auditor's approach in determining his audit strategy?'

According to Jenkins, Cooke and Quest (1992:18), the audit strategy describes the principal features of the proposed approach to the audit and it provides a basis for planning and controlling the subsequent audit work.

The factors that affect the audit strategy are (Jenkins et al., 1992:18):

- the objectives of the engagement;
- a review of the business to gain an understanding of it;
- an evaluation of the inherent risks that are associated with the engagement; and
- an initial assessment of internal control, including the overall control environment of the business, the principal features of the accounting system and the related internal accounting controls.

1.3 OBJECTIVES

The objectives of this short dissertation will be:

- to identify the risks -from an audit perspective- that are associated with the virtual enterprise; and
- to identify controls which the management of the auditor's client could implement to minimise these risks.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

The scope of this short dissertation will be limited to the objectives listed in 1.3 above. It will not attempt to identify all possible risks and controls to minimise these risks, but rather to give the auditor a framework from which he can work when assessing the risks from an audit perspective and the controls that could minimise these risks in a virtual enterprise environment.

Specifically, the following are excluded from this literature survey:

- The business benefits and drawbacks of the virtual organisation.
- The financial implications of the virtual organisation.

According to Grimshaw and Kwok (1998:46), there are many 'so-called' virtual organisations in the business environment today, but because they lack certain critical features, they are not considered virtual organisations, and are therefore excluded from this dissertation.

An example of these 'so-called' virtual organisations is (Grimshaw & Kwok, 1998:46): Companies that sell their products and services exclusively over the Internet, the teleshopping or telemarketing organisation.

The virtual enterprise has been defined for the purpose of this short dissertation in Section 2.5 of Chapter 2. In Chapter 3, the computer controls have been identified and classified according to SAICA's (South African Institute of Chartered Accountants) terminology, namely general CIS Controls and CIS application controls. However, the **detailed controls under each of these main category controls have not been** discussed here, as it is considered to be **beyond the scope** of this short dissertation. Furthermore, plastic cards, which are a prerequisite for certain EFT functions (e.g. EFTPOS and ATMs), are also **not discussed** in this short dissertation.

Chapter 4 identifies a framework to audit risks and controls in the virtual enterprise. As explained in Section 4.2.1, the whole virtual enterprise or one of the companies in the Virtual enterprise could be the auditor's client. Furthermore, the companies in the virtual enterprise could be using an integrated Enterprise Resource Planning (ERP) application system such as SAP R/3 System or various different applications that have interfaces to the main financial application. This short dissertation will however **not** explore these possibilities. Nevertheless, this research has opened these possibilities for further research.

1.5 DEFINITIONS

Before proceeding to the detailed aspects of this dissertation, it is important to offer certain essential definitions, which are central to this research topic:

1.5.1 Audit

The Oxford Paperback Dictionary defines 'audit' (the noun) as "official scrutiny of accounts" (Oxford University Press, 1996:48). It will be used in this context to describe the word approach, which is defined below:

1.5.2 Approach

The Oxford Paperback Dictionary defines 'approach' (the noun) as "act or means of approaching or technique" (Oxford University Press, 1996:35). In this context, it is used in conjunction with the word audit to give it a new meaning: audit approach.

According to Jenkins et al., (1992:2) the principal steps in carrying out the audit approach involve the following:

- Determination of the audit strategy;
- Understanding and recording of the system;
- Evaluation of internal control;
- Testing of controls and response to weaknesses; and
- Performing of substantive tests.

In this dissertation **audit approach** will mean:

- to identify the risks of an audit perspective that are associated with the virtual enterprise; and
- to identify controls which management of the auditor's client could implement to minimise these risks.

1.5.3 Risks

The Oxford Paperback Dictionary defines 'risk' (the noun) as "chance or possibility of danger, loss, injury, etc." Risk is also defined in this dictionary as "person or thing causing a risk or regarded in a relation to risk" (Oxford University Press, 1996:786).

SAAS 400 (SAICA, 1996) defines audit risk as follows:

"Audit risk" is the risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated. Audit risk has three components: inherent risk, control risk and detection risk.

"Inherent risk" is the susceptibility of an account balance or class of transactions to misstatement that could be material, individually or when aggregated with misstatements in other balances or classes, assuming that there were no related internal controls.

"Control risk" is the risk that a misstatement that could occur in an account balance or class of transactions and that could be material, individually or when aggregated with misstatements in other balances or classes, will not be prevented or detected and corrected on a timely basis by the accounting and internal control systems.

"Detection risk" is the risk that an auditor's substantive procedures will not detect a misstatement that exists in an account balance or class of transactions that could be material, individually or when aggregated with misstatements in other balances or classes.

In this short dissertation, the risks are mainly control risks and may have an effect on audit risk if not properly addressed.

1.5.4 Controls

The Oxford Paperback Dictionary defines 'controls' (the noun, used in plural) as "means of regulating" (Oxford University Press, 1996:183).

In this context, it will refer to controls as part of the company's internal control system. SAAS 400 (SAICA, 1996) defines 'internal control system' as follows:

"An "internal control system" consists of all the policies and procedures (internal controls) adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information".

1.5.5 Virtual

The Oxford Paperback Dictionary defines 'virtual' as "being so in practice though not strictly or in name" (Oxford University Press, 1996:1026).

In this context it is used in conjunction with 'enterprise', which is defined below:

1.5.6 Enterprise

The Oxford Paperback Dictionary defines 'enterprise' (the noun) as "undertaking, readiness to engage in such undertakings or business firm or venture" (Oxford University Press, 1996:289).

In this context, enterprise will refer to "business venture" and will be used in conjunction with the word 'virtual' to form a new term "virtual enterprise".

According to Grimshaw and Kwok (1998:46), the "term 'virtual organisation' is often known by other names- for example 'virtual *corporation'* (Davidow and Malone, 1992), 'virtual enterprise' (Cheng, 1996) or 'virtual *company'* (Fisher, 1993), though they all refer to the same concept". Grimshaw and Kwok (1998:46) states further that there is no consensus on the definition of the term 'virtual organisation'.

In this dissertation, the terms 'virtual enterprise' or 'virtual organisations' have been used; both refer to the same concept. The virtual enterprise as defined for the purpose of this short dissertation is discussed in detail in Section 2.5 of Chapter 2.

1.6 METHODOLOGY

Two separate literature surveys will be conducted in order to meet the objectives of this short dissertation:

- Chapter 2 will be devoted to a literature survey in order to identify the concept and attributes of the virtual enterprise, including the use of information technology in virtual organisations.

- Chapter 3 will also be devoted to a literature survey to discuss the audit risks and controls in a computer environment in order to develop a control model.

In Chapter 4, the control model developed in Chapter 3 for auditing risks and controls in a computer environment will be applied in order to develop a model or framework for auditing risks and controls in a virtual enterprise. Finally, Chapter 5 will conclude this short dissertation and indicate whether or not the objectives of this short dissertation have been met.

1.7 RESEARCH APPROACH

The research approach adopted in this short dissertation is to use the Control Model of Du Toit (1998) to develop a framework that can be used to identify the risks of a virtual enterprise and the related controls that will minimise these risks. In order to develop this framework, two literature surveys will be conducted, one in Chapter 2 and the other in Chapter 3.

1.8 SUMMARY OF RESULTS

The virtual enterprise, as defined for the purpose of this dissertation, was based on Grimshaw & Kwok's concept of the virtual enterprise and can graphically be displayed as shown in Figure 2.2 in Chapter 2.

In considering the risks and related controls in the virtual enterprise, the auditor will need to consider the **linkage between his/her client's internal network** (e.g. finance and accounting company's internal network) **and the external network, which involves the connection to the other companies in the virtual enterprise.** In considering this linkage and the related controls, it is clear that the *focus* would be on the **logical access** area as per the Computer Control Model (figure 3.4). However, due to the nature of the virtual enterprise, the auditor will have to consider, in addition to this, the **Internet risks and possibly the EDI/EFT risks (and the related controls) if a VAN is used.**

The framework for auditing risks and controls in the virtual enterprise has been documented in Table 4.1 in Chapter 4.

In summary, the auditor will need to consider the following when reviewing the risks and controls in the virtual enterprise:

- The CIS Environment of his/her client, consisting of both the CIS General (3.5.3.1) and Application Controls (3.5.3.2) using the Computer Control Model as depicted in Figure 3.4;

- The Internet Risks and the controls in place (3.6.2); and

- EDI and EFT Risks and the controls (3.6.1.2) if a VAN is used.

1.9 CONCLUSION

The objectives of this short dissertation have been met by providing a framework for the auditor to audit risks and controls in the virtual enterprise.

The framework will assist the auditor when evaluating the risks and controls in place in the virtual enterprise and also when recommending controls to the client's management if these controls are not in place.

This short dissertation has opened the following areas for further academic research:

- The risks and controls if an integrated enterprise resource planning (ERP) application is used for the virtual enterprise;
- The risks and controls if various different applications are used that interface to the main application in the virtual enterprise; and
- The effect on the audit approach if the whole virtual enterprise or only certain companies in the virtual enterprise constitute the auditor's client.

CHAPTER 2

THE VIRTUAL ENTERPRISE

CONTENTS PAGE

CHAPTER 2
THE VIRTUAL ENTERPRISE

2.1 OBJECTIVES

In general, the objectives of this literature survey are to obtain information and authoritative views on the concept of the virtual organisation, which can then be used as a basis for the construction of a model to assist in the evaluation of risks and controls in a virtual enterprise environment. In more specific terms, the objectives are:

- To obtain information and authoritative views on the concept and attributes of the virtual organisation; and
- To obtain authoritative views on the use of information technology in the virtual organisation.

2.2 NATURE OF THE LITERATURE SURVEY

In order to ensure the credibility and acceptability of the findings and proposals in this short dissertation, the views examined should be authoritative and generally accepted. An individual's views may be biased as a result of personal experience, the absence of formal research or knowledge of a particular computer environment. In order to prevent such bias, references have been restricted to those which had been released/ published by experts on the virtual organisation concept and to articles or research reports approved by recognised authorities in this field.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

The scope of this section of the literature survey will be to illustrate the concept and the attributes of the virtual organisation. The scope will also include the use of information technology in virtual organisations. The information so gathered will then be used, in Chapter 4, to identify the risks from an audit perspective that are associated with the virtual organisation.

Specifically, the following are excluded from this literature survey:

- The business benefits and drawbacks of the virtual organisation.
- The financial implications of the virtual organisation.

According to Grimshaw and Kwok (1998:46), there are many 'so-called' virtual organisations in the business environment today, but because they lack certain critical features, they are not considered virtual organisations, and are therefore excluded from this dissertation.

An example of these 'so-called' virtual organisations is (Grimshaw & Kwok, 1998:46): Companies that sell their products and services exclusively over the Internet, the teleshopping or telemarketing organisation.

2.4 BACKGROUND

The movement toward virtual enterprises is taking place in response to increasingly capable technology resulting in increased consumer access to information, reduced barriers to entry for competitors and increased customer mobility. The significantly more competitive environment that has emerged demands greater agility, responsiveness, cost effectiveness and focus from each enterprise, and demands extensive exploitation of each enterprise's core competencies (GartnerGroup, 1998:14).

"Becoming core-competency-centric enables an enterprise to achieve market excellence by narrowing its focus to doing those things it can do better than any competitor" (GartnerGroup, 1998:2).

GartnerGroup concludes by saying that the combination of enterprises narrowing their focus to become core-competency-centric and the need to offer a broader range of products and services has led to the emergence of the technology-enabled virtual enterprise.

According to Goldman et al., (1995:202) the virtual organisation is formed by integrating core competencies, resources, and customer market opportunities. He states that "It is dramatically better than business as usual for a network of companies sharing a business opportunity on a product and service basis."

Grimshaw and Kwok (1998:50) also share this view by proposing that the main criteria of the virtual organisation would be to have an organisation with many locations, the need to communicate between these locations by sharing information and work collaboratively on the shared information to produce joint products with the use of information technology as the facilitator.

2.5 THE CONCEPT OF THE VIRTUAL ORGANISATION

The traditional computerised organisation can be described as in figure 2.1:

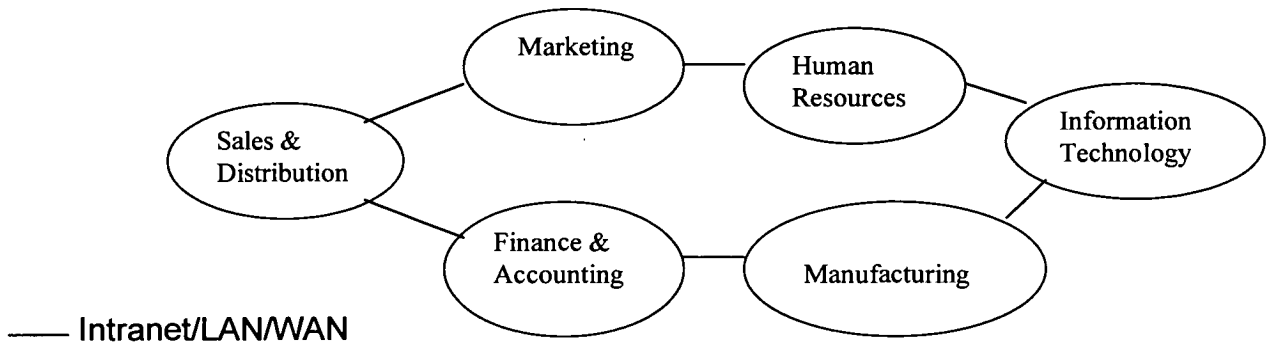

Figure 2.1: The traditional computerised organisation

In the traditional computerised organisation, as depicted in Figure 2.1, the organisational functions may all be linked together using an Intranet and a Local Area Network (LAN) or Wide Area Network (WAN).

What sort of organisation is the virtual organisation? Davidow and Malone (1992:5) tried to answer this question by explaining that to an outside person, "it will appear almost edgeless, with permeable and continuously changing interfaces between company, supplier, and customers". From the inside, the business will have traditional offices, departments and operating divisions that will constantly be reformed according to need (Davidow & Malone, 1992:6).

Goldman et al., (1995:233) view the concept of a virtual organisation as that of "an opportunity-based dynamic organisational structure" which is used to "bring pieces of a variety of organisations together to meet a worthwhile opportunity".

Palmer (1998:72) views the virtual organisation as an organisation that "behaves like" an existing organisation "by bringing together a set of resources: financial, material and human". He continues to propose that virtual organisations have a common goal, share information, and have incentives to cooperate, and can share resources.

Goldman et al., (1995:211) is of the opinion that there are six strategic reasons that motivate companies to adopt the virtual organisational model:

- Sharing infrastructure, research and development, risk and costs;
- Linking complementary core competencies;
- Reducing concept to cash time through sharing;
- Increasing facilities and apparent size;
- Gaining access to markets and sharing market or customer loyalty; and
- Migrating from selling products to selling solutions.

GartnerGroup (1998:3) view the virtual enterprise as "outsourced noncore competencies, a focus on a core strength or business, little or no physical presence or infrastructure, a network of business alliances, the exploitation of intellectual capital, and a heavy reliance on telecommunications".

Finally, perhaps Grimshaw and Kwok (1998:50) best define the concept of the virtual organisation as follows:

"..a group of companies forming an *alliance* through the use of *ICT* to *collaborate* in the production of a joint product; the location of the group of companies may be distributed locally or globally but appear to function as a single organisation".

The virtual enterprise, as defined for the purpose of this dissertation, is based on Grimshaw & Kwok's concept of the virtual enterprise and can be described as shown in Figure 2.2 on the following page.

Figure 2.2 illustrates the virtual enterprise as a *group* of companies forming an *alliance* using *information technology* and *communication* (either Internet or Extranet) to *collaborate* in the production of a joint product. The location of the companies may be local or global. Although the various organizational areas such as sales and distribution are referred to as various *companies*, these may also be sole proprietors, partnerships or even close corporations. *However, for the purpose of this dissertation, it is assumed that all the organizational areas such as sales and distribution will be companies as shown in figure 2.2.*

The reason why IT (information technology) is indicated in a dotted rectangle in figure 2.2, is that the IT function would not necessarily be required in the virtual enterprise in the sense of an IT Organization with programmers, analysts, etc. It will depend on various factors, for example, if in-house developed or off-the-shelf-applications are used in the virtual enterprise. In the case of off-the-shelf-applications, the applications would be supported by the vendor and not form part of the virtual enterprise as such.

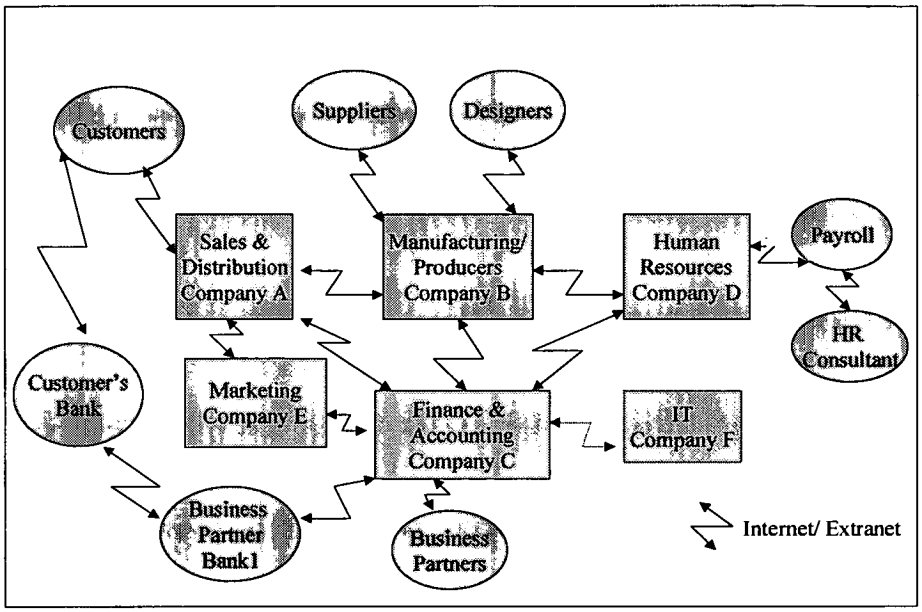

Figure 2.2: The Virtual Enterprise (derived from Grimshaw and Kwok's concept of the Virtual Enterprise)

Figure 2.2 also illustrates the virtual enterprise as "the combination of independent enterprises required to fulfil a defined customer need". GartnerGroup continues to propose that the virtual enterprise is logically and not physically defined (GartnerGroup, 1998:4).

As shown in Figure 2.2 above, the participating elements of the virtual enterprise are not owned by a single enterprise, but are all independent and form the virtual enterprise through an alliance.

2.6 THE ATTRIBUTES OF THE VIRTUAL ORGANIZATION

What are the characteristics that make a virtual organisation a virtual organisation?

Gallegos and Powell (1997:26) summarise the characteristics of the virtual organisation as follows:

- It employs a mass customisation strategy to produce high-quality, feature- and information-rich products;
- It maintains low cost with flexible programs such as JIT (just-in-time) and TQM (total quality management);
- It has a networked, team-orientated and distributed-decision-making organisational approach;
- The network is dynamic as it synthesises the best available capabilities and resources by linking designers, producers, suppliers, distributors and customers ; and
- It has teams that collaborate, regardless of their location and time zones; are granted important decision-making authority and foster openness, co-operation and trust among the network organisations and the people who comprise them.

According to Grimshaw and Kwok (1998:50), the essential attributes of the virtual organisation are:

- Alliance for a common goal;
- Underlying information and communication technologies (ICT);
- Vertical integration;
- Globalisation; and
- Collaboration.

Based on five case studies, Grimshaw and Kwok (1998:51) conclude the following about the above five attributes:

- **Collaboration:** Is a **necessary** feature of a virtual organisation and is often a prime motivational factor contributing to the formation of virtual organisations.

- **Globalisation:** Is a **necessary** feature of a virtual organisation and is often a prime motivational factor contributing to the formation of virtual organisations.

- **ICT:** Is a **necessary** feature, but not a sufficient feature and enables the formation of virtual organisations, but is not a motivational factor.

- **Vertical integration:** Is an **optional** feature of a virtual organisation in the sense that is not necessary for virtual organisations to have this attribute. The reasons for businesses to move towards vertical integration may be business process re-engineering and JIT.

- **Alliance:** Is an **optional** feature of a virtual organisation in the sense that is not necessary for virtual organisations to have this attribute. The motivation for businesses to move towards alliance may include the need to reduce the "product to market" time.

2.7 THE USE OF INFORMATION TECHNOLOGY IN VIRTUAL ORGANISATIONS

In a recent research survey conducted by Jonathan Palmer of the University of Oklahoma, regarding the use of information technology in virtual organisations, the respondents' responses to the important elements of their information infrastructure were (Palmer, 1998:76):

- 18% use mainframes;
- 98% use PCs;
- 89% use Local Area Networks (LANs);
- 40% use Wide Area Networks (WANs); and
- 93% use the Internet.

Palmer's research survey also revealed the following (Palmer, 1998:77):

- Fax and e-mail are regularly used;
- Intranet, videoconferencing, teleconferencing, groupware (e.g. Lotus Notes) and the Gopher site is also used, but very rarely; and
- World Wide Web sites were extensively used.

The use of the Internet and World Wide Web sites are not surprising, given the nature of virtual organisations and their need to connect to their partners in the virtual organizational structure.

The respondents in Palmer's survey were also generally positive about the impact of information technology on their operations and their ability to connect with their partners. In fact, 96% of the respondents agreed that information technology makes the virtual organisation more effective (Palmer, 1998:78).

2.8 CONCLUSION

This chapter has introduced the concept of the virtual organisation as viewed by various authors, and the way in which it is defined for the purpose of this dissertation. It has also revealed the five main attributes of the virtual organisation concept: alliance for a common goal, vertical integration, globalisation, collaboration and information technology.

In addition, the chapter has also illustrated the use of information technology in the virtual organisation. It was not surprising to see the very high usage of the Internet and World Wide Web by the virtual organisations in the survey, given the concept and attributes of the virtual organisation.

CHAPTER 3

AUDIT RISKS & CONTROLS IN A COMPUTER ENVIRONMENT

CONTENTS PAGE

CHAPTER 3

AUDIT RISKS & CONTROLS IN A COMPUTER ENVIRONMENT

3.1 OBJECTIVES

The previous chapter (Chapter 2) discussed the concept and attributes of the virtual enterprise, including the use of information technology in the virtual enterprise.

Chapter 3 will be devoted to a literature survey to discuss the audit risks and controls in a computer environment. In more specific terms, the objectives are:

- to establish a Control Model which can be used to audit risks and controls in a computer environment; and
- to determine whether or not the mentioned Control Model can be used in an EDI and or Internet Environment.

In the next chapter, the Control Model used in this chapter will be applied to develop a Control Model or framework to audit risks and controls in the virtual enterprise.

3.2 NATURE OF LITERATURE SURVEY

In order to ensure the credibility and acceptability of findings and proposals of this short dissertation, it is essential that the views examined be authoritative and generally accepted among computer auditing professionals. An individual's views may be biased as a result of personal experience, the absence of formal research or knowledge of a particular computer environment. In order to prevent such bias, references have been restricted to those which have been released/published by auditors and professional auditors' bodies.

3.3 SCOPE, LIMITATIONS AND EXCLUSIONS

The scope of this part of the literature survey will be as follows:

- The Path Context Model of Boshoff (1990), will be used to develop a Computer Control Model to address the risks and controls in a CIS environment;
- The computer controls will be classified according to SAICA's latest terminology (1998) and fitted into the Computer Control Model;
- However, the **detailed controls under each of these main category of computer controls have not been** discussed here, as they are considered to be **beyond the scope** of this short dissertation;
- Furthermore, plastic cards, which are a prerequisite for certain EFT functions (e.g. EFTPOS and ATMs), are also **not discussed** in this short dissertation.
- The risks and controls concerning the EDI/EFT and Internet environments will briefly be discussed;
- Both this chapter and the preceding chapter will form a foundation for Chapter 4.

3.4 BACKGROUND

In a fast-moving IT-dependent business world, the premium on effective control cannot be underestimated. Volume of transactions is on the increase, whereas speedy response times are invariably a commercial imperative. Automation has concealed activity and as a result there are fewer people employed which means less potential to observe, review and detect. More reliance has to be placed on automated auditing methodologies. With margins acutely under pressure in a highly competitive market, it is not easy for management to justify a generous resourcing of control and audit activity. Management will often be willing to adopt new, strategically important IT-based methods of conducting business with inherent control risks and fraud potential (Chambers & Rand, 1994:5).

3.5 ESTABLISHING A CONTROL MODEL

3.5.1 Background

According to the South African Institute of Chartered Accountants (SAICA) SAAS 401 "Auditing in a Computer Information Systems Environment", the overall objective and scope of an audit does not change in a CIS (Computer Information Systems) environment. The use of a computer changes the generation of transactions, processing, storage and communication of financial information and may affect the accounting and internal control systems employed by the entity.

SAAS 401(SAICA, 1998a) continues to state that the auditor should, as part of the planning phase of the audit, obtain an understanding of the significance and complexity of the CIS activities and the availability of data for use in the audit.

According to SAAS 401(SAICA, 1998a) this understanding includes the following:

- The organisational structure of the entity's CIS activities and the extent of concentration or distribution of computer processing and development throughout the entity, particularly as they may affect segregation of duties at both the user and CIS personnel levels;

- The significance of computer processing in each significant accounting application;

- The complexity of computer processing in each significant accounting application;

- Recent changes by the entity to replace or significantly amend a CIS where these changes will affect the internal control structure;

- Recent and planned changes to non-financial systems that may have an impact on the financial reporting of the entity in the reporting period; and

- The availability of data. Source documents and certain computer files may exist only for a short period of time or only in machine-readable form.

The risks and internal control characteristics in CIS environments include the following, according to SAAS 401 (SAICA, 1998a):

- Lack of transaction trails;
- Lack of segregation of functions;
- Potential for errors and irregularities;
- Initiation or execution of transactions;
- Dependence on other controls over computer processing (the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general CIS controls);
- Uniform processing of transactions. (Programming errors will result in all transactions being processed incorrectly); and
- Potential for increased management supervision. (CIS can offer management a variety of analytical tools which, if used, may enhance the internal control structure).

3.5.2 The Path Context Model

Before continuing with the development of the Control Model, it is necessary to describe the Path Context Model (PCM) of Boshoff (1990). Although the PCM was developed for mainframes, with slight adjustments it can be made applicable to any PC (Personal Computer), File Server or Midrange Computer as depicted in figure 3.1 below:

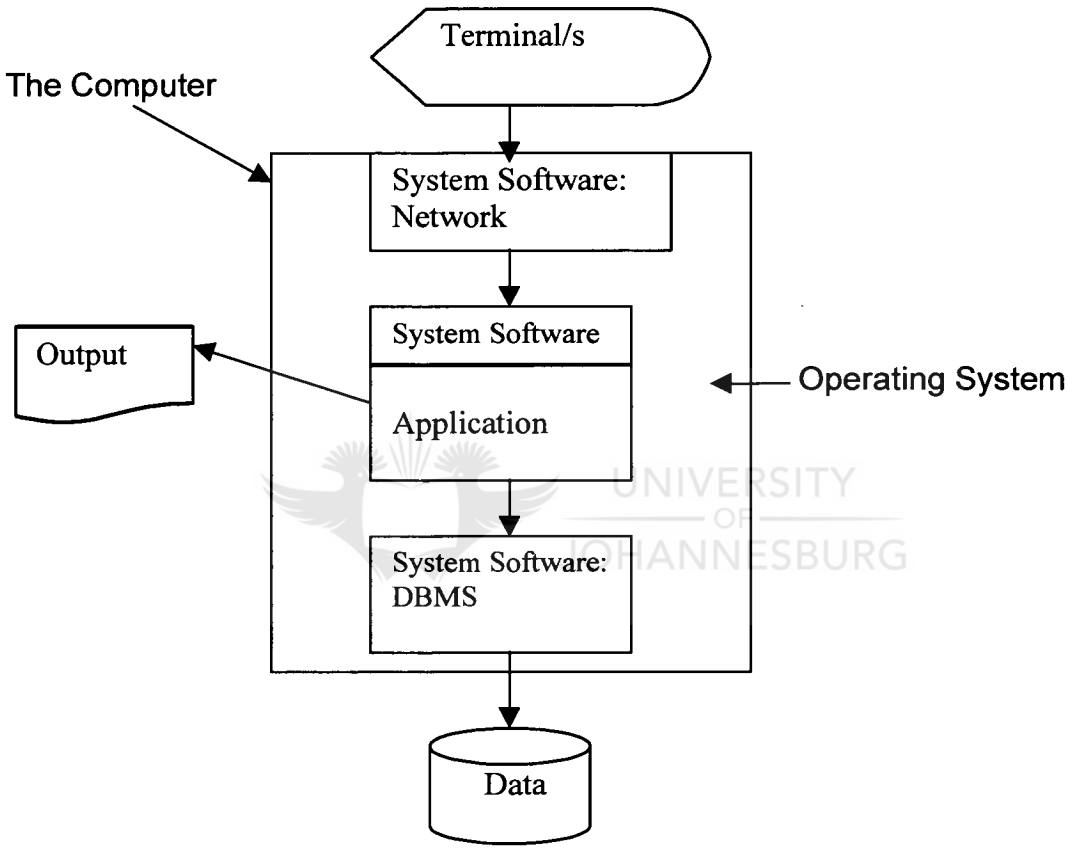

Figure 3.1: The Path Context Model (adjusted from Boshoff, 1990)

With reference to figure 3.1, in generic terms, a message from the keyboard or terminal will firstly encounter a network program (part of the system software) running under an operating system. Then the message will meet system software under which the application programs run (e.g. in a PC it might be Windows '95 or Windows NT). The message will then be routed to the application program (e.g. SAP R/3), which will instruct the database management system (DBMS) to read, write or copy data to or from the database on the hard drive (or any other magnetic storage media) from where it can be viewed on screen or on a printout (Du Toit, 1998:3).

3.5.3 Classification of controls

Before continuing to establish the Control Model, using the PCM, it is necessary to look at the classification of computer controls in order to fit all controls in a generic computer Control Model.

Computer Controls may be classified into two main areas, being **general controls** and **application controls** (Du Toit, 1998:2). Over the years, various names developed for these terms, for example, Information Technology (IT) controls and application controls (Jenkins et al., 1992:24). However, the South African Institute of Chartered Accountants (SAICA) 1998 terms will be used for the remainder of this dissertation as they represent the latest generally accepted terms.

According to SAAS 4011 (SAICA, 1998b) internal controls in a CIS environment consists of **general CIS controls** and **CIS application controls**.

3.5.3.1 General CIS Controls

SAAS 4011 (SAICA, 1998b) states that the "purpose of general CIS controls is to establish a framework of overall control over the CIS activities, and to provide a reasonable level of assurance that the overall objectives of internal control are achieved". SAAS 4011 sub-defines the general CIS controls into the following controls:

- **Organisation and management controls** (designed to establish an organisational framework over CIS activities), including:

  - appropriate policies and procedures relating to control (e.g. virus protection); and

  - segregation of incompatible functions.

- **Application systems development and maintenance controls** (designed to provide assurance that systems development and the maintenance thereof are done in an authorised and efficient manner), including controls over:

  - testing, conversion, implementation and documentation of new or amended systems;

  - access to systems documentation;

  - changes to application systems; and

  - acquisition of application systems from third parties.

- **Computer operation controls** (designed to control the operation of the systems), providing reasonable assurance that:

  - only authorised systems and programs are used, and access to computer operations is restricted to authorised personnel; and

  - processing errors are detected and corrected.

- **System software controls** (designed to ensure that system software is acquired or developed in an authorised and efficient manner), including:

  - authorisation, approval, testing, implementation of new systems software and systems software modifications; and

  - restriction of access of systems software and documentation to authorised personnel.

- **Logical access controls**, including:

  - access to data and programs is restricted to authorised personnel; and

  - an authorisation structure exists over transactions being entered into the system.

- **Disaster recovery controls** (designed to contribute to the continuity of CIS processing), including:

  - offsite storage of backup data and programs; and

- provision and recovery procedures for offsite processing in the event of a disaster.

Using the PCM of Boshoff and combining it with the terms of SAICA for the sub-categories of general CIS controls, the general CIS controls can graphically be displayed as in Figure 3.2 (as derived from Du Toit, 1998:5).

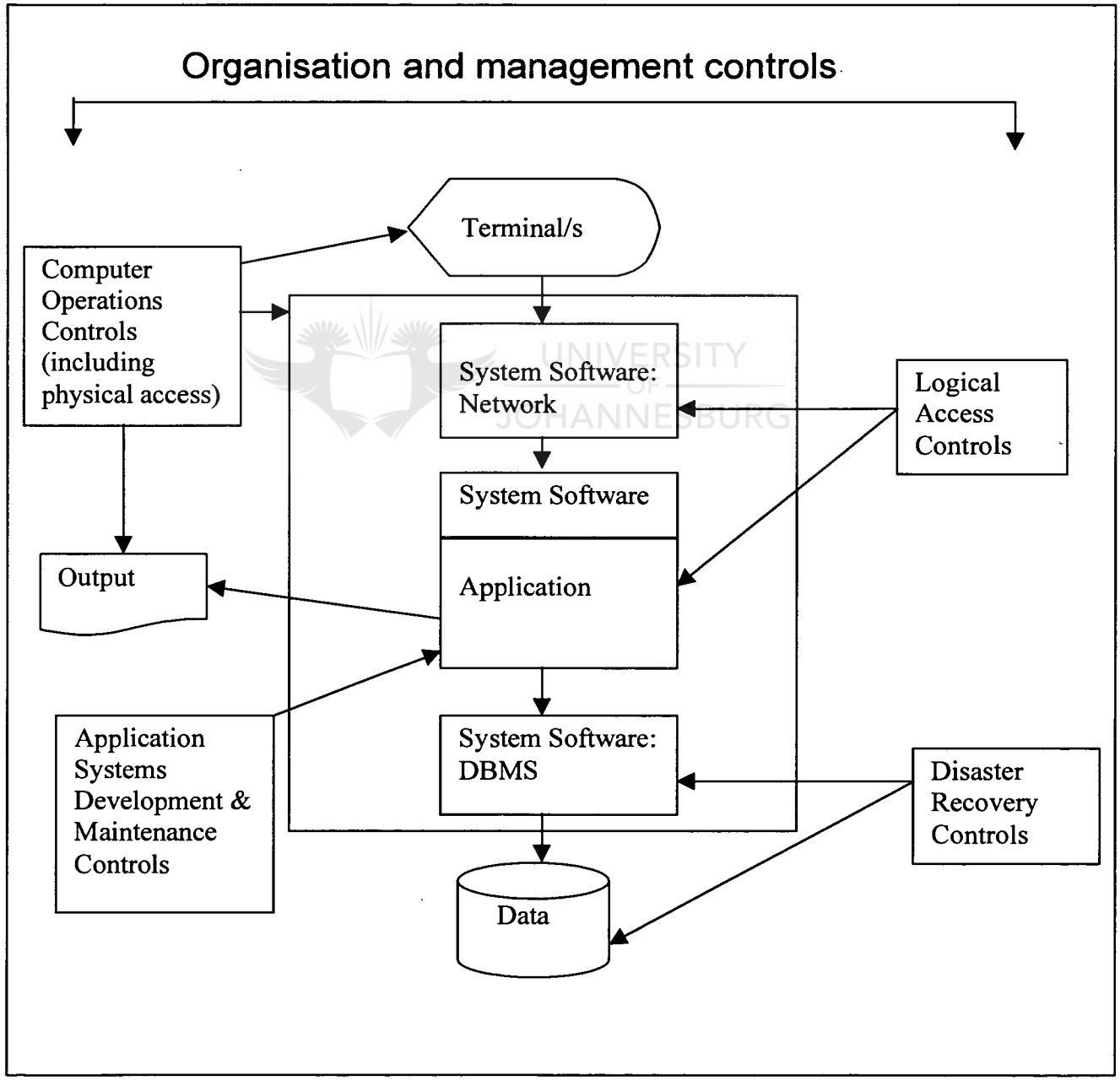

Figure 3.2: General CIS controls (as derived from Du Toit, 1998)

3.5.3.2 CIS Application Controls

According to SAAS 4011 (SAICA, 1998b) the "purpose of CIS application controls is to establish specific control procedures over the accounting applications in order to provide reasonable assurance that all transactions are authorised and recorded, and are processed completely, accurately and on a timely basis". SAAS 4011 divides the CIS application controls into the following:

- **Controls over input**, which provide reasonable assurance that:
  - transactions are properly **authorised** before being processed by the computer;
  - transactions are **accurately** converted into machine readable form and recorded in the computer data files;
  - transactions are not lost, added, duplicated or improperly changed **(completeness)**; and
  - incorrect transactions are rejected, corrected and resubmitted on a timely basis **(completeness and accuracy)**.
- **Controls over processing and computer data files**, which provide reasonable assurance that:
  - transactions, including system generated transactions, are **accurately** processed by the computer;
  - transactions are not lost, added, duplicated or improperly changed **(completeness)**; and

- processing errors are identified and corrected on a timely basis **(completeness and accuracy)**.

- **Controls over output**, providing reasonable assurance that:

  - processing results are **accurate**;

  - access to output is restricted to **authorised** personnel and provided to authorised personnel on a timely basis.

According to SAAS 4011 (SAICA, 1998b) the controls over input, processing, data files and output may be carried out by **users** or be **programmed** into the application software. In summary, when reviewing the CIS application controls, the auditor may wish to test the following (SAAS 4011, SAICA 1998b):

- **Manual controls exercised by the user** (if capable of providing reasonable assurance that the system's output is complete, accurate and authorised);

- **Controls over system output**; and

- **Programmed control procedures**.

Taking all of the above into account, and using the application portion of the PCM of Boshoff, the CIS application controls can graphically be displayed as depicted in Figure 3.3 (as derived from Du Toit, 1998:5):

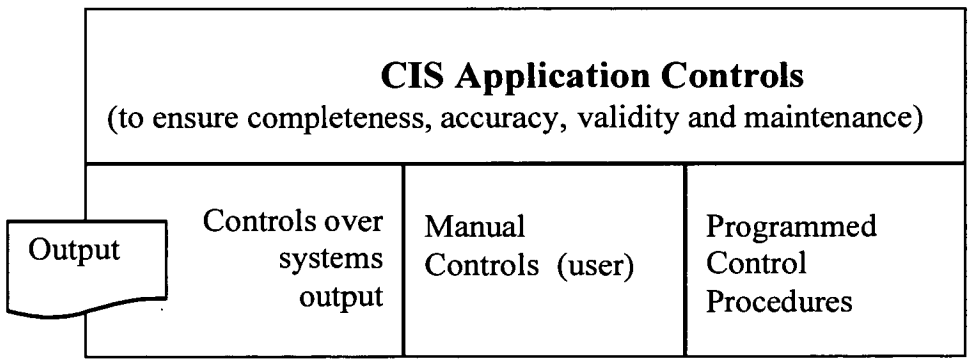

Figure 3.3: CIS Application Controls (derived from Du Toit, 1998)

3.5.3.3 Computer Control Model

Finally, after much discussion about the two CIS controls (being CIS general controls and CIS application controls), and using the Path Context Model of Boshoff, one can combine the two models into one representative model, the Computer Control Model. However, this model is valid only for any traditional computer system, being either mainframe or PC and located as stand-alone or part of the LAN (local area network) or WAN (wide area network), (Du Toit, 1998:6). Figure 3.4 represents the Computer Control Model.

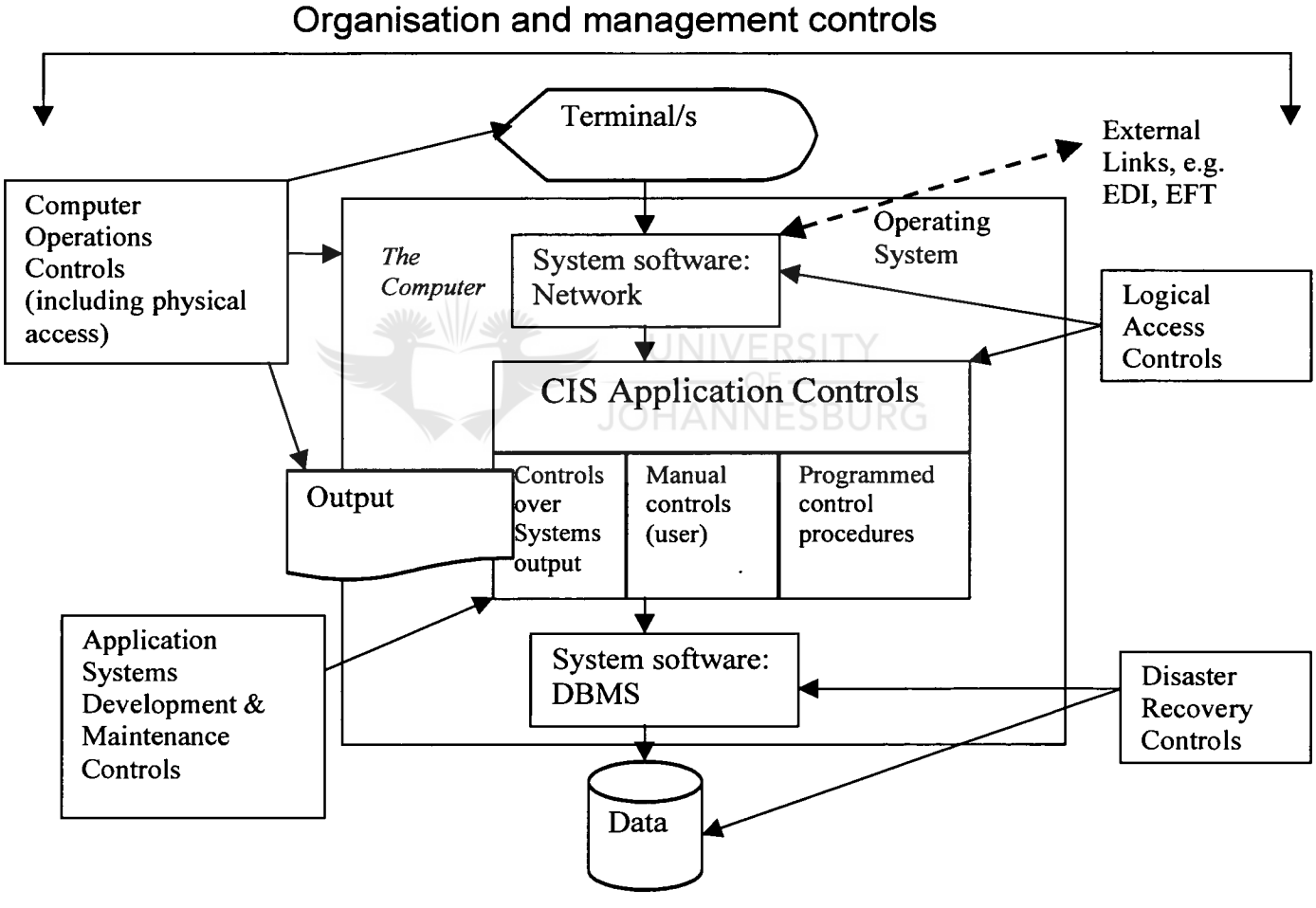

Figure 3.4 The Computer Control Model (derived from Du Toit, 1998)

3.6 EDI, EFT & INTERNET

3.6.1 EDI and EFT

3.6.1.1 Introduction

The Information Technology Series booklet, *Paperless Business Transactions (An introduction to the risks and controls)* (SAICA 1995), defines EDI as follows:

"ELECTRONIC DATA INTERCHANGE (EDI) represents the capability for one business partner to transact directly with another via their computer systems. It facilitates the direct transfer of business documents (transactions) and information between one or more business partners and other parties interested in these transactions".

Electronic funds transfer (EFT) is defined by Jenkins et al., (1992:481) as follows:

"Electronic funds transfer (EFT) is the initiation, approval and execution of payments and other transfers of funds using a computer network rather than paper".

Taking all of the above into account, EDI and EFT can graphically be displayed as in Figure 3.5 (derived from SAICA 1995) below:

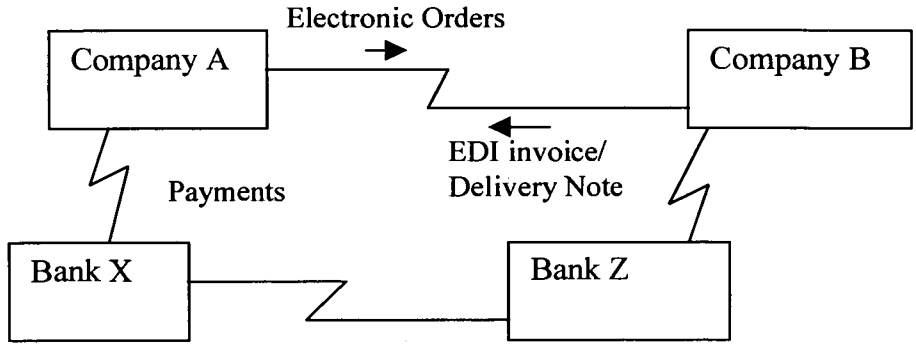

Figure 3.5 EDI & EFT (derived from SAICA, 1995)

In an EDI environment, third parties referred to as VANS (Value Added Networks) will often be responsible for maintaining the data communications network between the business partners. Such a scenario can graphically be displayed as in figure 3.6 below (derived from SAICA 1995):

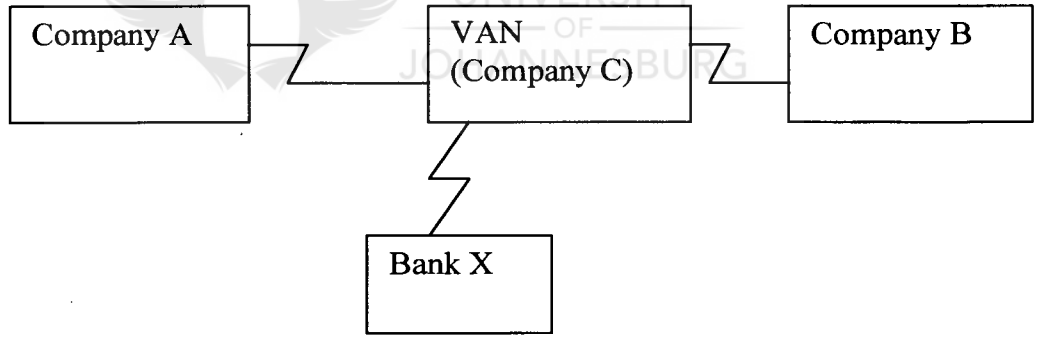

Figure 3.6 EDI with a VAN (derived from SAICA, 1995)

3.6.1.2 Risks and related controls associated with EDI and EFT

- **EDI**

According to the IT briefing booklet, *Harnessing EDI-Controlling the Business Risks* (The Institute of Chartered Accountants in England and Wales 1992), the most important risks and their related controls are as depicted in Table 3.1 below:

Risks	**Controls**
1. General Risks (are inherent to EDI) • Increased dependence on trading partners • Increased dependence on technology • Reduced human involvement • Dependence on service suppliers • Legal uncertainty	1. General Controls • Good trading partner relationships (formal legal agreement between business partners) • Re-appraise physical security , contingency and disaster recovery procedures • Access to high - quality management information • Legal Service Level Agreements with network service suppliers • Compliance with current legal and audit requirements

Table 3.1 Risks and related controls associated with EDI (derived from The Institute of Chartered Accountants in England and Wales, 1992)

2. Internal Risks (within an organisation's own control) • *Internal security failures*, including: Unauthorised access; Disclosure of confidential data; Failure of computer hardware and software; Infection by viruses; Loss of computing facilities due to fire; and Inadequate transaction trails. • *Implementation risk*, including: Failure to adapt existing controls to cope with EDI; EDI software which incorrectly translates data from internal applications to EDI message formats; and EDI software that cannot read all EDI messages. • *Processing risk*, including: Messages delayed or overlooked; or Messages incorrectly transferred to internal applications.	2. Internal Controls • Data Security policies and procedures should be reviewed and enhanced to include EDI risks • Appointing of an EDI specialist to co-ordinate implementation of EDI as well as training users in all aspects in the use of EDI in the business • Systems development and maintenance controls applied to EDI developments • Programmed and manual checks to ensure messages have been sent • Encryption and digital signatures used to authenticate incoming messages • Checks to reconcile number of messages received with transactions input into the applications • Acknowledgement of messages sent • Reviewing either manually or by the computer application itself, that the message is commercially sensible prior to passing it on to the main existing commercial system
3. External risks (under control of	3. External Controls (largely beyond

another party, e.g. network provider) • Trading partner's controls • Loss of confidentiality of sensitive information • Cross-border regulations • Loss or degradation of EDI service • Errors during transmission • Manipulation of messages during transit	the organisation's direct control) • Effective implementation of general and internal controls • Establishing good relationship with trading partners • Independent security audits on service supplier

Table 3.1(continue) Risks and related controls associated with EDI (derived from The Institute of Chartered Accountants in England and Wales, 1992)

- **EFT**

EFT has been defined in section 3.6.1.1 above. In an EFT environment there could be clearing and non-clearing functions involved in the transfer of funds, according to the IT Briefing booklet, *Moving Money -Electronic Funds Transfer Explained* (The Institute of Chartered Accountants in England and Wales 1992).

However, for the purpose of this dissertation, the **risks and related controls relating to ATMs (Automated Teller Machines) and EFTPOS (Electronic Funds Transfer at Point-of-Sale)** will be discussed briefly, as it is anticipated that these two non-clearing functions will *mostly* be involved in the virtual enterprise scenario.

Plastic cards, which are required for both ATMs and EFTPOS, will **not** be discussed here, as they do not form part of the scope of this dissertation. Electronic Banking uses Internet technology and will not be discussed separately.

According to the IT Briefing booklet, *Moving Money -Electronic Funds Transfer Explained* (The Institute of Chartered Accountants in England and Wales 1992), the most important system threats and countermeasures relating to ATM Networks and EFTPOS Systems, are as set out in Table 3.2 below:

Threat	**System Countermeasure**	**User Countermeasure**	**Perceived Level of Risk**
Customer PIN exposure to unauthorised persons:			
-careless or intentional	-	Customer must not disclose PIN	High
-via viewing of keypad	-	Customer must not allow bystanders to observe	High
- during transmission to host	Encryption of PIN	-	NIL
- storage of PINS at host	Encryption of all PINS at all times	Logical access controls over files	Minimal
Office service (i.e. no host authorisation)	Limitation on the amount which can be withdrawn and number of transactions per day	Check of customer signatures and card validity and genuineness	High
Exposure of PIN encryption keys	Transmission only in encrypted format under Master Keys	Controls over key management function Regular change	NIL

	Storage in ATM in tamper resistant environment	of keys	
Unsupervised ATM access	Automatic "off-line" status when back of ATM opened	ATM "off-line" during service	Low
Message amendment and deletion	Authentication, encryption and message sequence numbering	-	NIL
Fraudulent message request	Authentication, encryption and message sequence numbering	-	NIL
Fraudulent transaction creation and card capture	-	No usage of mail order type facilities with payment by card	High
Unauthorised use of the System	-	Strict controls over development and security Access controls over system resources and data	Minimal

Fraudulent use of lost and stolen cards	Blocking use of card and card capture	Notification of loss by customer	High

Table 3.2 System threats and countermeasures relating to ATM Networks and EFTPOS Systems (derived from The Institute of Chartered Accountants in England and Wales,1992)

3.6.1.3 The Computer Control Model

The Computer Control Model of Du Toit (1998) as depicted in figure 3.4 can be regarded as a single system because there are no outside users who have access to the system. The terminal/s as depicted in figure 3.4 may also be remote where communication controls (part of logical access controls) and to some extent, the system software controls, will require more emphasis (Du Toit, 1998:8).

However, the model is still valid in the EDI/EFT/EFTPOS/ATM environment where the model is "squeezed into one box or border representing one single system (called the ***client's*** system)" with linkages to other systems (Du Toit, 1998:8). For example in the EDI/EFT scenario as depicted in figure 3.6, the **client's system (Company A)** was linked to a VAN, which, in itself, is just another computer system with the same characteristics and controls as that of the client's system. As shown in figure 3.6 the business partner's computer (Company B) and the bank (Bank X), as another trading partner, are also linked to the VAN.

3.6.2 INTERNET

The Internet forms a massive electronic communications pipeline between businesses, consumers, government agencies, schools and other organisations worldwide, opening up new possibilities that challenge traditional ways of interacting, communicating and doing business (Price Waterhouse 1998:231).

It is not the purpose of this dissertation to discuss the Internet concept, but to identify briefly the risks that are associated with the Internet and the related countermeasures (controls) for these risks.

According to Young (1997), the **Internet risks**, which translate into risk for the organisation, are the following:

- Unauthorised access;
- Denial of Service (aimed at preventing the organisation from using its own computers);
- Information theft (e.g. using network sniffing); and
- Repudiation (one or more users participating in a transaction will deny participation).

Young (1997) demonstrates that typical services which are available on the Internet also pose risks to users who allow their use:

- **Electronic mail (E-mail)**- Forging of E-mail and the accepting of E-mail opens the enterprise up for denial of service attacks;

- **File Transfer**- Allowing users to use FTP (File Transfer Protocol) to transfer files and, by doing so, get unauthorised access to writable directories;

- **Remote Terminal Access and Command Execution** -Using Telnet for remote terminal access on the Internet is dangerous as Telnet sends all of its information unencrypted;

- **Usenet News** -Users might release confidential information or trust the information they receive or the denial of service risk; and

- **The World Wide Web (WWW)** - Uses the HyperText Transfer Protocol (HTTP) with two security risks: what a malicious client can do an enterprise's HTTP server and vice versa.

In considering the most important controls for an organisation that is linked to the Internet, one has only one important consideration: the linkage between the internal network (client's system) and the external network. It is clear that the only area that should be focused on is the **Logical Access** area, which involves **Security** to a large extent (Du Toit, 1998:13). The most important **control techniques or technologies used in Internet technology are:**

- A comprehensive **Internet Security Policy** should be in place and monitored by management, which addresses the following areas (Young, 1997):

  - **Internet Services** (for example which Internet services are allowed and guidelines regarding the use of these services);
  - **Security** (the definitions of security implementations, for example firewalls that will be used);
  - **Privacy** (the definition of the expected privacy regarding logging and monitoring issues);
  - **Access** (Policy statements regarding access rights and privileges of all users);
  - **Accountability** (the definition of responsibilities of users, administrators and management);
  - **Authentication** (the definition of policies regarding the use of authentication devices and remote location authentication);
  - **Availability** (the definition of user's expectation for the availability of Internet Services); and
  - **Violation** (the indication of which violations will be reported and to whom).

- **Firewalls** -A firewall is a mechanism used to protect a trusted network from an untrusted network. Typically, the two networks in question are an organisation's internal network (trusted) and the Internet (untrusted), (Young, 1997). The two main methods used by Firewalls of securing transmission to and from internal networks are packet filtering and proxy services (Young, 1997).

- **Encryption** of information/data to avoid unauthorised access, disclosure of information or denial of service (Oberholster, 1997). The main techniques used in encryption are (Oberholster, 1997):

  - Private key encryption;
  - Public key encryption;
  - RSA Algorithm;
  - Certification authorities and digital certificates; and
  - Key management.

- **Anti-virus protection** (Price Waterhouse 1998:373)

- **Authentication** with the use of SSL (Secure Sockets Layer), S-HTTP (Secure HyperText Transport Protocol) and TLS (Transport Layer Security) (Price Waterhouse 1998:375).

The Computer Control Model of Du Toit (1998) is still valid for the Internet, the only difference being that the VAN in figure 3.6 is replaced with an Internet Service Provider (ISP).

3.7 CONCLUSION

The objectives of this chapter have been met:

- A Computer Control Model (figure 3.4) was developed for all categories of computer controls for the traditional computer system; and
- It was also shown that the Computer Control Model remains valid for other computerised environments, EDI/EFT and Internet.

This chapter also highlighted some of the risks and related controls in an EDI/EFT and Internet environment.

Together with Chapter 2, a basis has now been established to develop a control framework or model that the auditor can use to audit the risks in a virtual enterprise environment.

CHAPTER 4

RISK/CONTROL MODEL FOR THE VIRTUAL ENTERPRISE

CONTENTS PAGE

CHAPTER 4

RISK/CONTROL MODEL FOR THE VIRTUAL ENTERPRISE

4.1 OBJECTIVES

In Chapter 1, the objectives for this short dissertation have been set to:

- identify the risks from an audit perspective that are associated with the virtual enterprise; and
- to identify the controls which the management of the auditor's client could implement to minimise these risks.

Chapter 2 was devoted to a literature survey to obtain information and authoritative views on the concept of the virtual enterprise as well as the use of information technology in the virtual enterprise.

Chapter 3 was also devoted to a literature survey to establish a Control Model which can be used to audit risks and controls in a computer environment and to determine whether the proposed Control Model can be used in an EDI and or Internet Environment. It was established that the Control Model remains valid for the latter with specific focus on the Logical Access controls to address the identified risks.

The objective of Chapter 4 will be to develop a Control Model or framework to audit risk and controls in the virtual enterprise by using the Control Model of Chapter 3 and the information in Chapter 2.

4.2 RISK/CONTROL MODEL FOR THE VIRTUAL ENTERPRISE

4.2.1 Introduction

In Chapter 2 the virtual enterprise has been defined for the purpose of this short dissertation as follows:

" The virtual enterprise, as defined for the purpose of this dissertation, is based on Grimshaw & Kwok's concept of the virtual enterprise and can be described as shown in Figure 2.2.

Figure 2.2 illustrates the virtual enterprise as a *group* of companies forming an *alliance* using *information technology* and *communication* (either Internet or Extranet) to *collaborate* in the production of a joint product. The location of the companies may be local or global. Although the various organisational areas such as sales and distribution are referred to as various *companies*, these may also be sole proprietors, partnerships or even close corporations. However, for the purpose of this dissertation, it is assumed that all the organisational areas such as sales and distribution will be companies as shown in figure 2.2".

In Chapter 3 the Computer Control Model of Du Toit (1998) as depicted in figure 3.4, represents **one single system, called the client's system** with all the controls still relevant but not shown when the model is extended to include linkages to other systems.

Figure 4.1 below represents a simplified graphic display if we combine the Virtual enterprise as in figure 2.2 with the Computer Control Model (figure 3.4).

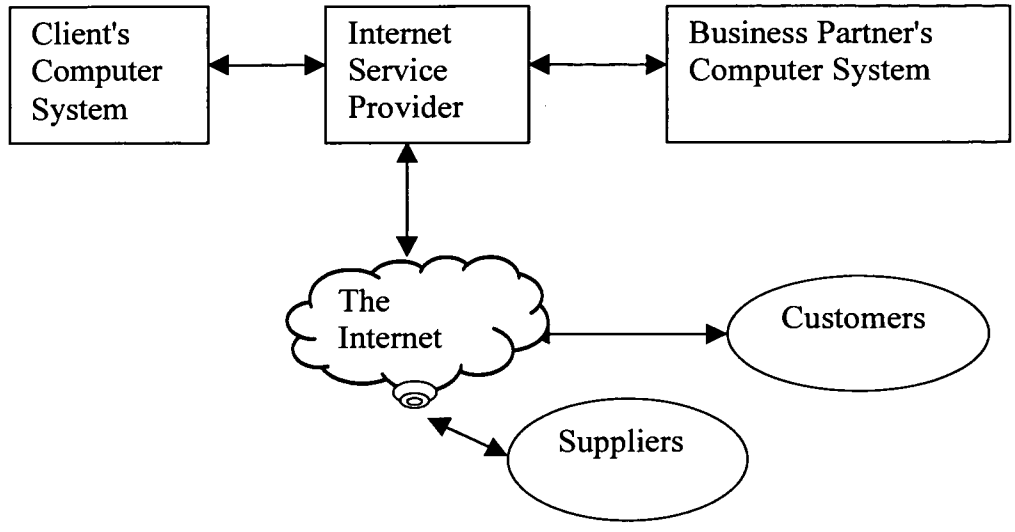

Figure 4.1: The virtual enterprise and computer control model simplified (derived from Du Toit, 1998 and figure 2.2 page 21)

As shown in figure 4.1, the Computer Control Model is "squeezed into one box or border" (called the ***client's*** system). In the virtual enterprise scenario, the client's system is linked via the ISP (Internet Service Provider) to the business partner's computer system. In comparing figure 4.1 to figure 2.2, the client's system could be (for example) the sales and distribution company (company A) and the business partner's system could be the manufacturing company (company B).

In a virtual enterprise scenario, the whole virtual enterprise or only one of the companies in the virtual enterprise (for example, the finance and accounting company) could be the auditor's client.

The virtual enterprise (being all the companies that forms part of the virtual enterprise *alliance*) could be using an integrated application system such as the SAP R/3 System, where one single integrated system is used for all the business areas. Alternatively, there could be various different application systems in use by the various companies in the virtual enterprise *alliance* (for

example, the sales and distribution system) that have interfaces to the main financial application system.

This dissertation will not explore all possible scenarios for the virtual enterprise as described above, as perhaps future research should do. However, this short dissertation will provide the auditor with a framework to audit risks and controls in the virtual enterprise.

4.2.2 Risk/Control Model for the Virtual enterprise

In considering the risks and related controls in the virtual enterprise, the auditor will need to consider the **linkage between his client's internal network** (for example, the finance and accounting company's internal network) **and the external network, which involves the connection to the other companies in the virtual enterprise.** In considering this linkage and the related controls, it is clear that the *focus* should be on the **Logical Access** area as per the Computer Control Model (figure 3.4). However, due to the nature of the virtual enterprise, the auditor will have to consider, in addition to this, the **Internet risks and possibly the EDI/EFT risks (and the related controls) if a VAN is used.**

In summary, the auditor will need to consider the following when reviewing the risks and controls in the virtual enterprise:

- The CIS Environment of his/her client, consisting of both the CIS General (3.5.3.1) and Application Controls (3.5.3.2) using the Computer Control Model as depicted in Figure 3.4;

- The Internet Risks and the controls in place (3.6.2); and

- EDI and EFT Risks and the controls (3.6.1.2) if a VAN is used.

Table 4.1 provides a framework which the auditor may use to identify the risks, and guidance on the controls that will address these risks in a virtual enterprise environment.

Risks	Controls or Control Techniques
1. CIS Environment	***1.1 General CIS Controls***
• Lack of transaction trails; • Lack of segregation of functions; • Potential for errors and irregularities; • Initiation or execution of transactions; • Dependence on other controls over computer processing; • Uniform processing of transactions; and • Potential for increased management supervision	• Organisation and Management Controls; • Application Systems Development & Maintenance Controls; • Computer Operation Controls; • System Software Controls; • Logical Access Controls; and • Disaster Recovery Controls. ***1.2 Application Controls (to ensure completeness, accuracy, validity and maintenance)*** • Manual Controls exercised by the user; • Controls over system output; and • Programmed control procedures.
2. Internet • Unauthorised Access; • Denial of Service; • Information Theft; and • Repudiation	• Comprehensive Internet Security Policy; • Firewalls; • Encryption; • Authentication; and • Anti-virus protection.

Risks	Controls or Control Techniques
3. EDI	
• Increased dependence on trading partners • Increased dependence on technology • Reduced human involvement • Dependence on service suppliers • Legal uncertainty • *Internal security failures* including: Unauthorised access; Disclosure of confidential data; Failure of computer hardware and software; Infection by viruses; Loss of computing facilities due to fire; and Inadequate transaction trails. • *Implementation risk*, including: Failure to adapt existing controls to cope with EDI; EDI software which incorrectly translates data from internal applications to EDI message formats; and EDI software that cannot read all EDI messages. • *Processing risk*, including: Messages delayed or overlooked; or Messages incorrectly transferred	• Good trading partner relationships (formal legal agreement between business partners) • Re-appraise physical security , contingency and disaster recovery procedures • Access to high - quality management information • Legal Service Level Agreements with network service suppliers • Compliance with current legal and audit requirements • Data Security policies and procedures should be reviewed and enhanced to include EDI risks • Appointing of an EDI specialist to co-ordinate implementation of EDI as well as training users in all aspects in the use of EDI in the business • Systems development and maintenance controls applied to EDI developments • Programmed and manual checks to ensure messages have been sent • Encryption and digital signatures used to authenticate incoming messages

Risks	Controls or Control Techniques
to internal applications. • Trading partner's controls • Loss of confidentiality of sensitive information • Cross-border regulations • Loss or degradation of EDI service • Errors during transmission • Manipulation of messages during transit	• Checks to reconcile number of messages received with transactions input into the applications • Acknowledgement of messages sent • Reviewing either manually or by the computer application itself, that the message is commercially sensible prior to passing it on to the main existing commercial system • Effective implementation of general and internal controls • Establishing good relationship with trading partners • Independent security audits on service supplier

Table 4.1 (continue) Risk/Control Framework for the Virtual Enterprise

Risks	Controls or Control Techniques
4. EFT (EFTPOS and ATMs only)	
• Customer PIN exposure to unauthorised persons: -careless or intentional -via viewing of keypad -during transmission to host -storage of PINS at host • Office service (i.e. no host authorisation) • Exposure of PIN encryption keys • Unsupervised ATM access • Message amendment and deletion • Fraudulent message request • Fraudulent transaction creation and card capture • Unauthorised use of the System • Fraudulent use of lost and stolen cards	• Customer must not disclose PIN • Customer must not allow bystanders to observe • Logical access controls over files • Check of customer signatures and card validity and genuineness • Controls over key management function • Regular change of keys • ATM "off-line" during service • No usage of mail -order type facilities with payment by card • Strict controls over development and security • Access controls over system resources and data • Notification of loss by customer • Encryption of all PINS at all times • Limitation on the amount which can be withdrawn and number of transactions per day • Transmission only in encrypted format under Master Keys • Storage in ATM in tamper-resistant environment • Automatic "off-line" status when back of ATM opened

Risks	Controls or Control Techniques
	• Authentication, encryption and message sequence numbering • Blocking use of card and card capture

Table 4.1 (continue) Risk/Control Framework for the Virtual Enterprise

4.3 CONCLUSION

The objectives of this chapter have been met, namely, to develop a framework, which the auditor can use to evaluate the risks and controls in the virtual enterprise.

Although the framework is not an exhaustive one, it will nevertheless give the auditor a framework from which to work. As technology changes over time, it will be necessary to revise and re-evaluate this framework by means of future research.

CHAPTER 5

CONCLUSION

The objectives of this short dissertation have been met as a framework to audit risks and controls in the virtual enterprise has been developed.

The framework will assist the auditor when evaluating the risks and controls in place in the virtual enterprise and also when recommending controls to the client's management if these controls are not in place.

Before the present research project, knowledge of the virtual enterprise environment - specifically concerning the risks involved and how these risks will effect the auditor - was limited and anecdotal. It is hoped that the present research, specifically concerning the auditor, has contributed towards a better understanding of the risks and the controls that would minimise these risks.

This short dissertation has opened the following areas for further academic research:

- The risks and controls if an integrated enterprise resource planning (ERP) application is used for the virtual enterprise;
- The risks and controls if various different applications are used that interface with the main financial application in the virtual enterprise; and
- The effect on the audit approach if the whole virtual enterprise or only certain companies in the virtual enterprise constitute the auditor's client.

BIBLIOGRAPHY

ANDERSON, M. & SMITH A.C. 1998: IEW Scenario: Virtualizing the office. GartnerGroup.

BOSHOFF, W.H. 1990: A Path Context Model for computer security phenomena in potentially non-secure environments. Johannesburg: Rand Afrikaans University (D. Comm thesis).

CHAMBERS, A. & RAND, G. 1994: Auditing the IT environment: Assessing and measuring risk and control. London: Pitman Publishing.

DAVIDOW, W.H. & MALONE, M.S. 1992: The virtual corporation: Structuring and revitalizing the corporation for the 21st century. New York: Harper Collins Publishers.

DU TOIT, A. 1998: Controls related to the Internet and Electronic Commerce. Southern African Accounting Association Biannual Congress (1998: Johannesburg).

GALLEGOS, F. & POWELL, S.R. 1997: Telecommunications networks in virtual corporations. IS Audit & Control Journal, Vol. 3, 1997: 26-28.

GOLDMAN, S.L.; NAGEL, R.N. & PREISS, K. 1995: Agile competitors and virtual organisations-Strategies for enriching the customer. New York: Van Nostrand Reinhold.

GRIMSHAW, D.J. & KWOK, S.F.T. 1998: The business benefits of the virtual organisation. (In: Igbaria, M.; Tan, M. eds. 1998: The virtual workplace. Idea Group Publishing).

JENKINS, B.; COOKE, P. & QUEST, P. 1992: An audit approach to computers. London: The Institute of Chartered Accountants in England and Wales.

MCNEE, B. & SCHLIER, F. 1998: The virtual enterprise- The phenomenon that it built. GartnerGroup.

OBERHOLSTER, O. 1997: An audit model for the analysis and evaluation of encryption with reference to RSA. Johannesburg: Rand Afrikaans University (M. Comm dissertation).

OXFORD UNIVERSITY PRESS 1996. New York: The Oxford Dictionary of current English.

PALMER, J.W. 1998: The use of information technology in virtual organisations. (In: Igbaria, M.; Tan, M. eds. 1998: The virtual workplace. Idea Group Publishing).

PRICE WATERHOUSE (1998). Technology Forecast: 1998. Menlo Park, California: Price Waterhouse Technology Centre.

SAICA (South African Institute of Chartered Accountants). (1995) Paperless Business Transactions-An introduction to the risks and controls. January 1995. The South African Institute of Chartered Accountants.

SAICA (South African Institute of Chartered Accountants). (1998a) SAAS 401 Auditing in a Computer Information Systems Environment. April 1998. The South African Institute of Chartered Accountants.

SAICA (South African Institute of Chartered Accountants). (1998b) SAAS 4011 Risk assessments and internal control-Computer information systems characteristics and considerations. April 1998. The South African Institute of Chartered Accountants.

THE INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES. (1992a) Harnessing EDI-Controlling the business risks.

THE INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES. (1992b) Moving money -Electronic funds transfer explained.

YOUNG, B.C. 1997: Auditing validity on the Internet with specific reference to firewalls. Johannesburg: Rand Afrikaans University (M. Comm dissertation)