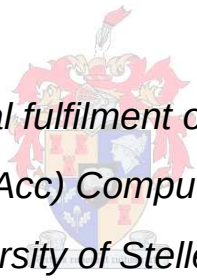
B2B AND THE SUPPLIER: PREVENTING

REPUDIATION OF ORDERS

IN AN OPEN ACCOUNT SYSTEM

by

RIKA BUTLER



Thesis presented in partial fulfilment of the requirements for

the degree M(Acc) Computer Auditing

at the University of Stellenbosch

Supervisor: PROF W BOSHOFF

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

Department of Accounting

December 2003

DECLARATION

I, the undersigned, hereby declare that the work contained in this thesis to be my own original work and that I have not previously, in its entirety or in part, submitted it at any other university for a degree.

R BUTLER

October 2003

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

1 Background and Statement of problem

"A buyer must not be able to place an order, thereby causing the seller to invest time and resources in filling that order, and then repudiate the order." (Romney & Steinbart, 2003: 61)

The risk of repudiation, as mentioned above, forms part of the three fundamental characteristics, namely "validity, integrity and privacy", that must be present in any business transaction. This includes e-business processes. (Romney & Steinbart, 2003: 61)

In B2B environments where customers are allowed to place orders on "open" accounts, the suppliers of the items are, among others, subjected to the particular risk of an unauthorised order being placed on the "open" account of an existing customer. This is possible in instances where a person illegitimately uses valid customer identification details (like user names and passwords), to place unauthorised orders. Another risk associated with the above, is the risk of unauthorised changes being made to a B2B order, after the initial approval and authorisation of the transaction.

In instances where either of the above occurred the customer will, at subsequent delivery of the goods, either deny placing the order, or disagree with the content of the delivery. The customer will refuse to accept the goods and consequently deny the responsibility of payment for the items involved – the customer has repudiated the transaction. Repudiation causes monetary losses to the supplier who had, based on the order it received, manufactured, packed, transported and delivered

the goods.

In this particular environment, specific internal control measures to verify the validity of a B2B order before being accepted and processed are necessary within the supplier's system. It is essential that the supplier establishes and verifies the source of an order and links it to a specific customer. It must be ensured that a valid customer placed the order and that it can be accepted and processed by the supplier without the risk of subsequent repudiation. The supplier must also have procedures in place to ensure that no unauthorised changes are made to previously approved order transactions, resulting in orders being filled and delivered inaccurately.

2 Purpose of study

The purpose of this study is to evaluate existing control frameworks and internal control measures in an attempt to provide a framework of internal control measures that can be implemented by B2B suppliers to address the risk of repudiation when orders are placed on open accounts.

If B2B suppliers implement the necessary controls it should lead to an improved system of internal control. It will decrease the occurrence of repudiation due to invalid orders that were accepted and processed, or processed whilst containing unauthorised changes. Less repudiation of transactions by customers should lead to the prevention or reduction of losses suffered by suppliers as a result thereof.

Suppliers operating in this environment can use the framework provided in this report to perform an assessment of their own systems of internal control. It will enable them to identify any weaknesses in their existing system of internal control and where necessary, make adjustments for improvement by implementing the controls recommended in the framework.

The framework can also assist auditors in their assessment of the

systems of internal control of audit clients falling within the identified category.

3 Methodology

To arrive at this framework of internal control measures, internal control and the purpose of a system of internal control will be discussed in Chapter 2. The specific problems and risks addressed in this report are also illustrated.

Chapter 3 provides a simplistic explanation of how a typical sales transaction transpires. Examples of the internal control measures that can be implemented to address the risk of repudiation within a manual system of internal control are mentioned. The sales process is then "translated" to a computer environment by describing how a typical sales transaction takes place when a computer is introduced. Typical internal control measures that can be implemented within a computerised system are briefly mentioned.

The Internet, e-business and B2B transactions are defined in Chapter 4. E-business risk and the problems associated with repudiation and the prevention thereof, is discussed. The term "open" B2B account system is explained.

Existing control frameworks and internal control measures available to address the risks associated with an e-commerce system are defined Chapter 5. These internal control measures are evaluated to determine which of these controls are relevant in a B2B environment to address the particular risks as defined. These internal control procedures are provided in Chapter 6.

A framework of internal control measures that will address the risks and problems associated with repudiation will be provided by way of a matrix in Chapter 7. A summary of this report and the conclusions drawn are provided in Chapter 8.

4 Limitations of study

Although the basic principles and the definition of internal control are provided in this report, it will be accepted as stated for purposes of this study and will not be examined or questioned further.

A typical purchase and payment cycle poses numerous business risks for both the buyer (customer) and the seller (supplier). This study will only address the repudiation-problem from the perspective of a B2B supplier, and only those related to orders for physical products. Although some of the concepts and risks may well be present in the environment that forms the topic of this report, Internet sales of digital and electronic products, like ShareWare, as well as the provision of services, fall outside the scope of this report.

The study will further be limited to B2B open account systems. Traditional e-business sales transactions where the creditworthiness and payment for the goods are immediately, electronically verified by the supplier, does not form part of this study. In such instances the supplier is not subjected to the specific risk as defined in this report. These types of systems once again creates additional risks, like the provision of stolen credit card information, the hacking of credit card information while being sent over communication channels, etc., that are not addressed in this report.

Lastly, although the purpose of this study is to provide a framework of internal control measures for these B2B suppliers, this report is not intended to be a document in which the technical issues regarding the functioning of these internal control measures are discussed.

CHAPTER 2

RISKS AND INTERNAL CONTROL

1 Business risks

When any transaction takes place between two business partners, risks are created when rights and obligations change hands. The Canadian Institute of Chartered Accountants (CICA) defines a risk as “any process, activity or event that can negatively influence the successful, sustainable and ethical achievement of enterprise objectives” (CICA, 1998: 409). According to King Report on Corporate Governance, “Risks are uncertain future events that could influence the achievement of an organisation’s objectives. These include risks threatening strategic, operational, financial and compliance objectives”. Risks should not only be viewed from a negative perspective.“ According to Suzanne Labarge, the Chief Risk Officer of the Royal Bank of Canada, “risk in itself is not bad, what is bad is risk that is mismanaged, misunderstood, mis-priced on unintended” (Naidoo, 2002).

A business risk is defined as “the likelihood that an organisation will not achieve its business goals or objectives” (Hunton, Bryant, Bagranoff, 2004: 48).

These enterprise or management objectives include aspects like:

- The effectiveness and efficiency of operations,
- Safeguarding the company’s assets,
- Compliance with applicable laws, regulations and supervisory requirements,
- Supporting business sustainability under normal, as well as adverse operating conditions,
- Reliable reporting, and

- Behaving responsibly towards all stakeholders. (King Report, 2002 and SAICA).

A specific risk exists “as a result of a location or method of operation of a particular function” (CICA, 1998: 8). Examples of critical risks a company may have to face are those relating to reputation, ethics, e-business, health, safety, environmental risks, as well as financial risks (KPMG, 2001). Risk varies according to the circumstances a company finds itself in. Both internal and external factors may contribute to the possibility of a risk occurring (Hunton, et al., 2004: 48). The risks a company is faced with are also influenced by the industry within which the company operates. New risks are introduced as companies change their business processes and models, like for example moving from a pure manual system to a system that is fully computerised.

Due to the fact that risk may vary from industry to industry, as well as within each business cycle, one particular type of transaction, namely a sales transaction taking place between two business partners, was chosen as the topic for further study.

When a sales transaction takes place the supplier (seller) incurs costs in the manufacturing, packaging and delivery of the goods, as soon as a sales order is approved and accepted. On delivery of the goods, the customer (buyer) is responsible for the monetary value or cost of the items delivered.

Based on the above definitions, it follows that risks will be present in and also arise from this sales process. Examples of the more general risks that can arise during a typical sales transaction is that unauthorised orders are processed, that orders are never processed, that orders are not executed and delivered accurately, that although ordered, goods are never sent to or never reaches the customer, etc.

2 The purpose of internal control

To address the business risks that are present within any transaction

cycle, the necessary internal control measures, or a so-called system of internal control, should be implemented. Various institutions have, by applying different control models, developed control frameworks (like CoCo, COSO and Cadbury) that can be applied to design a sound system of internal control. According to COSO (Committee of Sponsoring Organisations) one of the two principles of its efforts was to provide a standard against which businesses and other entities can assess their control systems and determine how to improve them (Boynton, Johnson & Kell, 2002: 324).

The COSO report (Internal Control – Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 1992) defines internal control as "a process, effected by the entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives …" (Boynton, et al., 2002: 325). CICA defines internal control as "those elements of an organisation (including its resources, systems, processes, structures and tasks) that, taken together, support people in the achievement of the organisation's objectives. Control is effective to the extent that it provides reasonable assurance that the organisation will achieve its objectives reliably" (CICA, 1998: 11).

Two of the important deductions that can be made from the above definitions of internal control need mentioning. Firstly that, due to the inherent limitations of internal control, a system of internal control can be expected to provide only reasonable assurance, and not absolute assurance, that if implemented, business risks would not materialise. The second is that the primary responsibility for the implementation and maintenance of this system of internal control lies with the directors and management of a company, while other parties (like the internal and external auditors) may also contribute useful information to an organisation in effecting control. (Boynton, et al., 2002: 325-328).

This primary responsibility of the directors relating to internal controls, are supported by the King Report on Corporate Governance in South Africa. According to King the directors of a company need to identify the

key risk areas and key performance indicators of a company as well as how those risks are to be managed. King states that the board must see to it that there are adequate internal controls in place and that the management information systems can cope with the strategic direction in which the company is headed.

3 Risk management

The extent of internal control measures necessary to address the risks present within business processes, are assessed as a result of a risk management process. The board is responsible for the total process of risk management, as well as forming its own opinion on the effectiveness of the process. Management is accountable to the board for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the company (King Report, 2002).

Risk assessment for a company is the process of:

- Identification of risk,
- Identification of its potential impact on the enterprise,
- Identification of existing controls which mitigate the risk,
- An evaluation of the adequacy of the existing controls, and
- The acceptability of the residual risk.

“Residual risk is the nett risk that remains after implementing controls to mitigate the impact of risk facing an enterprise.” (CICA, 1998: 9)

According to Protiviti, an American company that provides exclusive services on the areas of risk consultation and internal audit, the business risk management process is a continuous process of:

- Establishing risk management objectives, tolerances and limits for all of the enterprise’s significant risks,
- Assessing risks within the context of established tolerances,

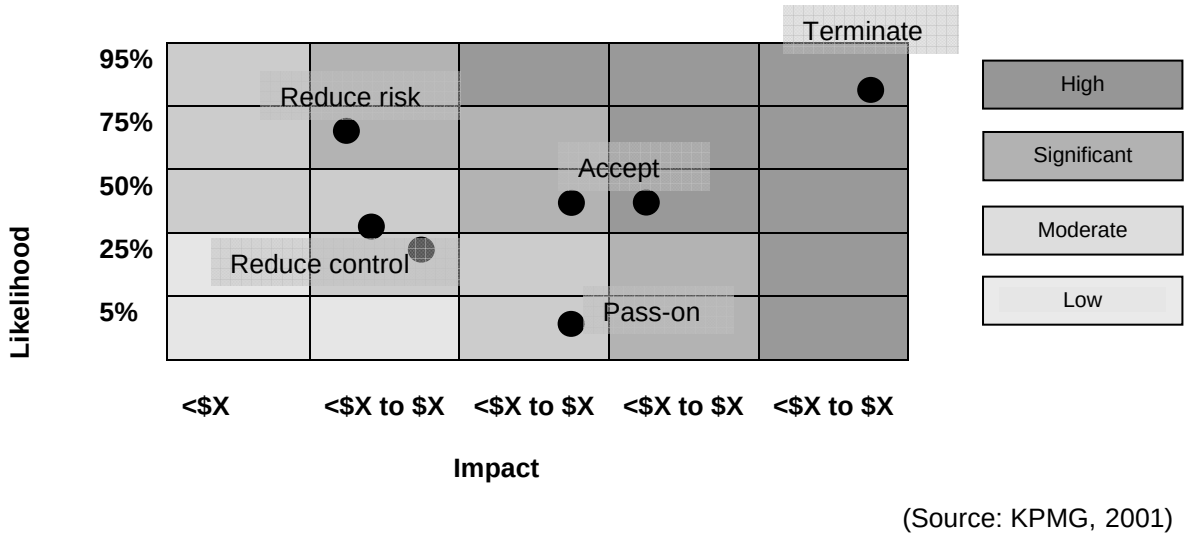
- Developing cost-effective risk management strategies and processes consistent with the overall goals and objectives,
- Implementing risk management processes,
- Monitoring and reporting upon the performance of risk management processes,
- Improving risk management processes continuously, and
- Ensuring adequate communication and information for decision making. (Protiviti, 2003)

KPMG defined Enterprise Risk Management (ERM) as a “structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value”. ERM maintains that a defined number of failures can be tolerated if the cost of guarding against them is more expensive than the risk they pose.

During this risk management process the probability that a risk will occur (“likelihood”), as well as its impact if it does occur (“magnitude”), are considered. As a result of this process some risks will require no action, while risks with a potentially high likelihood of occurrence as well as a material impact if it should occur, requires action of management to bring the risk within the acceptable range of risk, or to eliminate the risk altogether. This takes place based on the risk/benefit analysis of the effect of the action on the enterprise as a whole. (KPMG, 2001)

“In most situations, some residual risk is desirable, as the cost of implementing additional controls to eliminate the residual risk will exceed the potential impact of the residual risk occurrence” (CICA, 1998: 9). The board must decide on the company’s appetite or tolerance for risk – those risks that it will take and those it will not take in the pursuit of its goals and objectives (King Report, 2002).

The abovementioned process can diagrammatically be presented as follows:



(Source: KPMG, 2001)

Figure 1: Business Risk Matrix

In terms of the King Report the board is responsible for ensuring that a systematic, documented assessment of the processes and outcomes surrounding key risks is undertaken at least annually. This risk assessment should address the company's exposure to at least the following:

- Physical and operational risks,
- Human resource risks,
- Technology risks,
- Business continuity and disaster recovery,
- Credit and market risks, and
- Compliance risks. (King Report, 2002)

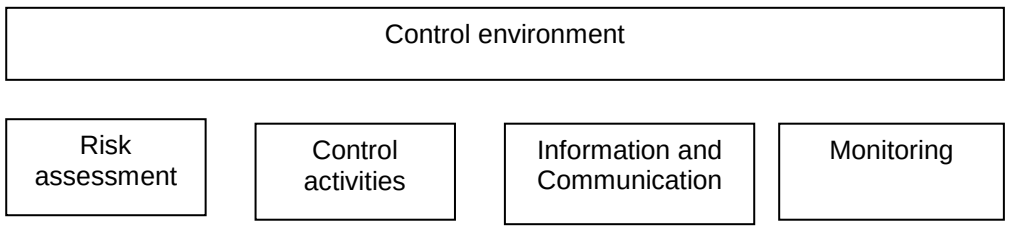
4 A system of internal control

The board should make use of generally recognised risk management and internal control models and frameworks in order to maintain a sound system of risk management and internal control to provide reasonable assurance regarding the achievement of organisational objectives. (King Report, 2002)

The COSO report identifies five interrelated internal control structure components, namely:

- Control environment,
- Risk assessment,
- Information and communication,
- Control activities, and
- Monitoring (Boynton, et al., 2002).

These components of a sound system of internal control can be presented as follows:



(Source: Arens & Loebbecke, 2000)

Figure 2: Components of internal control

It is important to note that the basic principles and the definition of internal control as presented and explained in this chapter will be accepted for purposes of this study.

CHAPTER 3

RISK OF REPUDIATION AND SPECIFIC INTERNAL CONTROL MEASURES

1 Risk of repudiation for supplier

One of the major business risks that a sales transaction poses to the supplier is the risk of repudiation of the transaction by the customer. In the context of a sales transaction taking place between a supplier and a customer and taking standard dictionary definitions into account, repudiation comprise that a customer (at delivery of the goods) denies, refuses or renounces his/her commitment or obligation towards the supplier. As mentioned previously this causes financial losses to the supplier, who had invested resources, time and effort into fulfilling the order.

Repudiation of an order by a customer may be the result of:

- Unauthorised orders that were placed, unbeknown to the customer, while using his/her details, and/or
- Discrepancies between what was originally ordered and what are being delivered. This might be the result of unintentional mistakes made by the supplier, or intentional unauthorised changes made to the order after it was initially approved and accepted by the two parties involved.

In order to minimise the possibility of repudiation the supplier needs to verify that an order is authorised and valid (comes from whom it claims to come) before being accepted and executed. The supplier also needs to ensure that the details of the delivery agree with the order that was originally placed. Ensuring the validity of a transaction before being accepted, as well as ensuring no unauthorised changes between authorising and delivery of an order will therefore contribute to

minimising the risk of subsequent repudiation.

This is also evident from an explanation of the three characteristics of any business transaction, as stated by Romney & Steinbart. According to Romney & Steinbart any business transaction has to contain three characteristics, namely validity, integrity and privacy. It is defined as follows:

- Validity: Both parties to a transaction must be able to authenticate the identity of the other party to ensure that the transaction is valid and enforceable. A buyer must not be able to place an order, thereby causing the seller to invest time and resources in filling that order, and then repudiate the order. Conversely, a seller cannot be allowed to solicit orders and then renege on delivery.
- Integrity: Both parties to a transaction must have confidence that the information exchanged is accurate and has not been altered during the transmission process.
- Privacy: The privacy or confidentiality of business transactions and any information exchanged in those transactions must be maintained, if so desired by either party. (Romney & Steinbart, 2003: 61)

This risk of repudiation substantially increases in systems where goods are sold to customers on credit. The reason for this is that, in a credit system, payment for the items does not immediately take place on delivery of the items, but at some future stage, as agreed upon by the parties involved. In addition, the occurrence of unauthorised orders placed within a credit system might only be detected at a later stage, for example when the items are delivered to the customer, or when the customer receives an invoice or statement for payment.

It should be clear from the above that to sufficiently address the repudiation-risk it is essential that the supplier, before an order is accepted, authorised, processed and delivered, confirm the two important aspects, namely:

- The validity of the transaction and the source from which it came, as well as
- The integrity of the transaction - ensuring no unauthorised changes were made subsequent to the authorisation and acceptance of the order.

This can be achieved by implementing appropriate internal control measures to sufficiently address the specific risks associated with repudiation (Chapter 2).

2 Internal control measures within a manual system

In traditional manual business processes, authorisation and approval, which are usually principally evidenced by means of signatures, play an important role in ensuring the validity of a transaction. Additional procedures “such as signatures across sealed envelopes and certified or hand delivery” ensure that the contents of a message have not been altered. (Romney & Steinbart, 2003: 61)

The manual internal control measures that a supplier can implement to address the defined risk, usually involves that the customer signs the order as evidence of acknowledgement of placing the order and accepting the responsibilities arising from it. Where sales are made on credit, the creditworthiness of a customer will be checked before an order is accepted and processed. This ensures that a valid, signed “contract” exists between the customer and the supplier for the ordering of the items as specified in the order. Responsibility and authorisation of the order is thus determined and defined.

Before goods are sent to a customer, it is first established that an approved order exists (authorisation and validity) and that the content of the goods to be delivered agrees with what was originally ordered (integrity of the transaction). In practice this is achieved by agreeing the physical goods with copies of the order (in both the warehouse and the dispatch department’s possession), as well as the delivery note. This

process will amongst other things, confirm both the validity and authorisation for the dispatch, as well as detect any unauthorised changes made to originally, approved orders.

Upon delivery, the customer is required to sign a copy of the delivery note. This signed copy with which the customer acknowledges that the goods, as specified on the delivery note, were taken into possession is sent back to the supplier. Invoicing by the supplier can subsequently take place based on the original order (which was signed and approved by the customer) as well as the customer signed copy of the delivery note (evidence of receipt of the goods). With his/her signature, the customer indicates or acknowledges his/her responsibility or obligation towards the supplier.

When the internal control measures referred to in the preceding paragraphs are implemented, it reduces the risk that a customer can deny either placing the order or receiving the goods. Thus, no uncertainty exists regarding pinning responsibility for the monetary value of the items ordered and received on the customer.

3 Risks within an electronic environment

The principles of risks and internal control measures within a manual system as referred to in the preceding chapter are still applicable when the supplier operates within a computerised environment. The specific risks surrounding repudiation as defined earlier, still exists within an electronic environment. Romney and Steinbart states that the three fundamental characteristics of business transactions discussed previously, namely “validity, integrity and privacy”, are particularly true of e-business transactions (Romney & Steinbart, 2003: 61).

Although the utilisation of computerised systems hold many advantages for the parties involved, the use of new technology also (besides the various existing risks) introduces “new” and in some instance, even greater, business risks (Moscove, 2001 and Hunton, 2004: 2) that needs to be addressed by the parties involved. It was mentioned in Section 1 of

Chapter 2 that “new” risks originate as business processes and models change – which is the case when moving from a manual to a computerised system. Note that some of the “new” risks in a computer environment might be similar to problems experienced within a manual system, but are “new” as they have to be addressed in a different way.

Examples of these “new” risks that might be present in a computerised environment are using programs that contain programming errors, making mistakes during the input process, unauthorised access and changes to information, etc. It is important to note that although these, as well as numerous other risks are present within a computer environment, only the problems as defined earlier will be addressed in this report.

4 Importance of IT-governance

The Information Systems and Audit Control Association (ISACA) is of the opinion that when a computer is involved, it is critically important to the survival and success of an organisation to effectively manage information and related Information Technology (IT). IT Governance is defined by ISACA as “a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes”. (COBIT, 2000: 5)

The objectives of IT Governance are “to set strategies for IT so that it is closely aligned with organisational goals and use IT for the maximum opportunity but minimum risk”. IT Governance is therefore divided into two parts:

- The use of IT to promote an organisation’s objectives and to enable business processes, and
- Managing and controlling IT-related risks (Hunton, et al., 2004: 2).

It is thus clear that a supplier operating within a computer environment has to effectively manage and control their IT activities. This means that

they have to implement the necessary control measures in order to sufficiently address the risks they are facing.

5 Internal control measures within the computer environment

In section 2 of this chapter, the internal control measures that will assist in addressing the repudiation risk within a manual system were illustrated. As the environment in which a business operates and/or the technology utilised in the business process change, so the internal control measures have to be adapted in order to still effectively address risk (both the existing as well as the new risks created by the change).

The control measures necessary to address the repudiation-risk within a computer environment will greatly depend on the level of computerisation of the supplier's system. In systems were the computer is only used on a small scale some form of manual- and/or user controls might be sufficient, whilst applicable computerised internal measures might be essential in more complex computer systems.

Except in systems where no hard copy order exists (real-time systems), it is general business practice that the customer still signs the order (produced by the computer system), as a means of acknowledgement and pinning responsibility. Certain supplier's credit sales systems can even verify the debtor's account number, as well as the available credit of a customer automatically against the debtors' master file, before a credit order for goods is accepted and processed. This means that the customer's signature may still remain the main source of authorisation and ensuring the validity of an order. Alternatively, electronic verification as illustrated above can be used.

In a computerised system, the goods are still (as in a manual system) compared to the details of the copies of the order (which might only exist in an electronic format) before delivery takes place. Alternatively, the details of the goods dispatched are entered into the supplier's computer system, where it is automatically matched with the details of the order received. With this process authorisation for the goods to leave the

premises and the delivery to take place is established. Possible unauthorised changes made to orders will also be detected.

As in manual systems, customers are still required to sign and return signed delivery notes to the supplier. The details of the order, items dispatched and accepted by the customer can subsequently be entered onto the system of the supplier to be matched before invoicing takes place. Once again, the signature is acknowledgement of receiving the goods.

Due to the fact that in such systems, invoicing only takes place based on the matched details of the underlying documents (which links the responsibility for the transaction to a specific customer by way of a signature), the chances of the customer repudiating the transaction and denying of the responsibility thereof, is greatly reduced.

CHAPTER 4

THE INTERNET, E-BUSINESS, E-COMMERCE AND B2B OPEN ACCOUNT SYSTEMS

1 The Internet, e-business and e-commerce

A major development in the information systems domain during the early 1980's, was the emergence of the Internet. The Internet consists of a worldwide system of computer networks through which computer users can communicate and transfer information using a universal protocol, called TCP/IP (Transmission Control Protocol/Internet Protocol). (Weber, 1999: 989).

As computer technology evolved it became possible to conduct business transactions via the Internet - goods could be sold and bought over the Internet. The term e-business refers to all uses of advances in information technology with a view to improve the ways in which an organisation performs its business processes (Romney & Steinbart, 2003: 49).

E-business can be used for the following main types of activities:

- Advertising products to potential on-line shoppers by displaying product catalogues on websites,
- Electronic data interchange (EDI), where business information is shared and transferred between parties, in a data format understood by the parties involved,
- Electronic fund transfers (EFT), where funds are transferred from one person or entity's account to another in a paperless environment, by for example using Internet banking services,
- Business to consumer (B2C) transactions, where business transactions takes place via the Internet directly between the

consumers and suppliers, for example Amazon.com who sells books to on-line Internet users, and

- Business to business (B2B) transactions, where goods, services and/or information is shared between two business partners.

Weber defines electronic commerce (e-commerce) as “the use of technology to enhance the processes of commercial transactions among a company and its customer and business partners” (Weber, 1999: 991). This means that e-commerce is a narrower concept than e-business that refers only to the electronic execution of business transactions such as buying and selling via the Internet (Romney & Steinbart, 2003: 49).

Some industries are becoming increasingly dependent on technology for their survival, basically forcing them to change their business processes to include conducting business via the Internet. As a result of this and due to the various advantages it brings, e-commerce over the Internet is still increasing. Vendors, business partners as well as on-line retail shoppers find greater selection, convenience and lower prices on the Internet. By selling products over the Internet the potential customer base of a company is expanded substantially to millions of potential customers worldwide, which can be reached 24 hours of the day. It can lead to better satisfaction of the customer’s individual needs and can even bring about cost savings for the companies involved.

According to reviews (Wagner, 2000) it was estimated that about 200 million people worldwide were connected to the Internet in 2000. They were, at that stage, joined by seven new Internet users every second. Wagner predicted that by 2005 the Internet users were expected to have multiplied to one billion – one-seventh of the world’s population. (Wagner, 2000)

According to a study conducted by eMarketer in April 2000, almost 34 million US households were actively using the Internet, and of that number 23,5 million or 69% have made an Internet purchase. At that stage ActivMedia Research estimated that e-commerce activity for 2000 would amount to $132 billion worldwide. (AICPA, 2001)

Closer to home, the “Electronic Communications and Transactions Bill” as approved by the South African Parliament, came into effect on 1 March 2002. One of the aims of this Bill was “to provide for the facilitation and regulation of electronic communications and transactions …” The Bill is the first to acknowledge and give documents signed with electronic signatures the same legal status as signed paper documents in South Africa, thereby lending legitimacy to the e-commerce trade in South Africa.

2 Business to business (B2B) commerce

The concept of business partners conducting business among one another via the Internet (B2B-commerce) took the business world by storm in 1999 (Ward, 2003). Various companies integrate to form one, big, meta-company. Companies link their software, systems are integrated, and transactions and information is transferred between the companies concerned. With B2B the emphasis is on participation, the sharing of information and integration.

A further development on the B2B scene was the creation of exchanges by groups of related companies for the purpose of conducting transactions mutually and sharing information between the parties involved. The purpose of these exchanges is “… to create liquidity in fragmented markets, by matching bids and offers and by acting as neutral enforcers of the rules” (Williams, Dale, Visser & Van der Wiele, 2001) as well as to share information in a more collaborative way (Ward, 2003). Exostar is an example of such an exchange that was created by large players in the aerospace and defence industry (Ward, 2003).

The advantages of B2B commerce include the rapid availability of information, reductions in inventory levels, shorter manufacturing cycles and reduction in costs. Steve Butler, a senior analyst at eMarketer, alleges that the top players in the B2B industry are savings between 20% and 30% on their online transactions compared with traditional methods of conducting business (Ward, 2003).

The first major development is this area started when major firms such as Walmart and General Electric moved buying and selling online to cut costs and speed up supplies. General Electric reported (The Economist, 4 March 2000: 85-86) that due to this initiative procurement cycles was cut in half, processing costs by one-third and the cost of goods purchased by between 5% and 50%. In 1999 IBM had included 6,700 suppliers into its online procurement system and bought more than $12 billion worth of goods over the Internet, thereby eliminating around 5 million invoices. This, together with sharper purchasing as a result of increased transparency, etc., resulted in IBM saving $240 million on the $11 billion it spend. (Williams, et al., 2001)

Both Ford en General Motors reported in November 1999 that they were creating online automotive trade exchanges. At this stage, Ford, through a site called AutoXchange, planned to conduct $80 billion in transactions annually. By connecting to its 30,000 production suppliers it forecasted that through B2B transactions costs of conducting business could be cut by between 10% and 20% for the participating parties. Accordingly, General Motors, through a similar site, TradeXchange, believed that the cost of each purchase order would be slashed from $100 to $10. (Wagner, 2000)

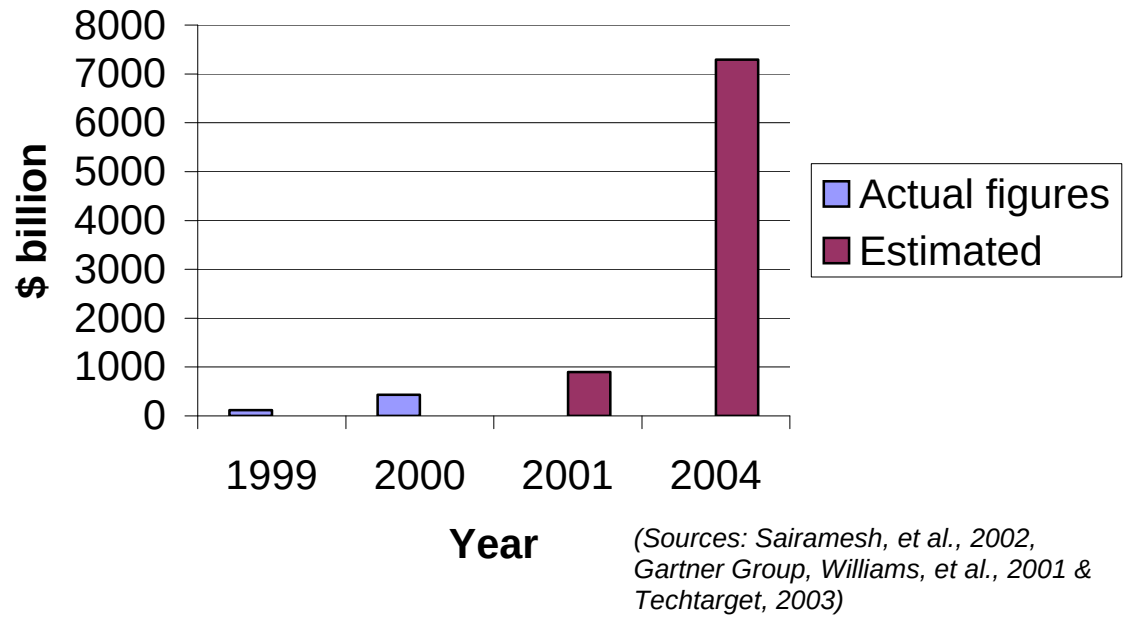
General Motors, Ford and Daimler Chrysler merged their individual exchanges in 2000 to create Covisint, a virtual market place for the automotive industry. According to a study by Goldman Sachs (Financial Times, 14 June 2000), the result would be a cost saving averaging just over $1000 per vehicle. (Williams, et al., 2001)

The Economist (26 February 2000) reported that in 1999 global e-commerce was worth little over $150 billion, with around 80% of these transactions taking place between one business and another (B2B) (Williams, et al., 2001). The popularity of B2B e-commerce is growing at a steady pace (Sairamesh, Mohan, Kumar, Hasson & Bender, 2002). Research in a study named “Real Numbers E-Commerce Study Series”, the result of which was published by ActivMedia Research in 2000, found that the extent of B2B purchasing was increasing and that the

volume of transaction would probably double over the next two years (that is until 2002). The study further found that 50% of all businesses then (in 2000) purchased online (Bartlett, 2000). Forrester reported (2 June 2000: 156) that 79 percent of large companies is expected to be trading online by 2002 (Williams, et al., 2001).

In a study performed by The Business Software Alliance (BSA), chief executive officers of various of the world's top technology companies indicated that a big future awaits B2B e-commerce and they predicted that by 2010 B2B e-commerce will be the most significant form of business transaction in terms of dollar value (Bartlett, 2001).

B2B commerce has created a global digital economy involving very substantial amounts of money. The value of B2B online transactions conducted has been escalating since first introduced in 1999 and is estimated to increase steadily, as illustrated below.



(Sources: Sairamesh, et al., 2002, Gartner Group, Williams, et al., 2001 & Techtarget, 2003)

Figure 3: Statistics to illustrate significance of B2B commerce

3 E-business risk

All of the concerns and objectives (which were applicable to normal business transactions) still apply to e-business transactions. It was previously mentioned that technology changes brought with it numerous opportunities and benefits, but also subjected businesses to new and in some instance, even greater, business risks (Moscove, 2001). As discussed earlier, risk changes as business models and processes change and IT-governance becomes essential, especially in the new e-commerce environment.

As B2B transactions can easily amount to thousands, millions and even trillions of dollars (as indicated earlier), sound security and governance is essential (Williams, 2001). The reason for this is that “failure … can prove massively expensive - financial repercussions can be astronomical, legal entanglements limitless and the effect on business partners incalculable” (Williams, 2001). An effective business strategy, which also addresses information technology, has to be developed and implemented (Moscove, 2001). E-business risk management, where e-business risk is identified and appropriately addressed by implementing the necessary internal control measures, is essential.

According to Moscove e-business risk can be classified into four categories, namely:

- Information technology infrastructure,
- User identification and authentication,
- User privacy, and
- Destructive computer programs.

The Internet has changed the way in which two parties interact with one another. Firstly, the parties involved in an Internet transaction might not know each other prior to the transaction. The parties might know little or nothing about each other’s true identity, address, creditworthiness, reliability, etc.

As a result, when e-commerce transactions take place via public

networks like the Internet, three fundamental problems arise (Weber, 1999: 991), namely:

- "How do the parties to a transaction establish each other's identity and authenticity?
- How do the parties to a transaction protect the privacy of their dealings?
- How do the parties to a transaction effect a secure exchange of money for any goods and services provided?"

The abovementioned is also supported by the three fundamental characteristics of e-business transactions - validity, integrity, and privacy, discussed earlier.

It is thus clear that the identification and confirmation (authentication) of a potential customer, as well as ensuring the integrity of a transaction (no unauthorised changes), is essential for all e-commerce transactions, as it is for any business transaction taking place manually or using computer technology. An important reason for this is to ensure that the transaction cannot subsequently by repudiated by the customer.

4 Non-repudiation in a digital environment

While all of the concerns and objectives present within a manual system, still apply to e-business transactions, the "methods used to satisfy them" (that is the internal control measures that can be implemented), do however change as technology evolves. (Romney & Steinbart, 2003: 61). This means that the risk of repudiation still exists in a digital environment, but that the controls necessary will differ from those that were appropriate and sufficient in a manual environment.

Non-repudiation within a digital environment requires that neither the sender not the receiver of a message be able to deny the transmission of a message (Stallings, 1995: 5). It means that "when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can

prove that the message was in fact received by the alleged receiver" (Stallings, 1995: 11).

Due to the fact that the supplier and the customer (or other business partner in case of B2B transactions) can geographically be separated from one another by thousands of kilometres when orders are placed via the Internet, the order can not *physically* be signed by the customer (as was the case in a manual system). This means that there is a lack of acknowledgement of placing the order, as well as a means in which to link the customer to the details of an order. No written 'contract', signed by the various parties as evidence of acknowledgment and accepting the conditions of the order, and the rights and obligations associated with it, is available.

As a result of the above two important risks are created in a digital environment, namely the risks that:

- Unauthorised orders, that was places by gaining authorised access, be accepted and processed, and
- After initially accepting the order, unauthorised changes are made to the order, due to unauthorised access being gained to the order before/while being sent over the Internet communication channels.

In an attempt to prevent repudiation in this environment it is necessary that an e-commerce order transaction (before being accepted and processed) be made legally binding and thus enforceable by the parties involved. To achieve this two important principles are necessary, namely:

- User identification, and
- User authentication.

CICA defines these two principles as follows:

- "User identification is the means by which users of information technology identify themselves when interacting with technology. Most often, this is a unique identifier, such as a logon or login-ID …"

- “User authentication is the means by which a user is confirmed as being the valid owner of the user identifier that the user presents to the system …“. (CICA, 1998: 219)

In most systems user identification and authentication is performed when a user logs onto the system. Techniques that allow for continuous user authentication during a session, to confirm that the user who logged on at the commencement of the session continues to be the one using the system, are available. Due to the sensitive nature of certain transactions it may be necessary to use additional authentication techniques to authenticate the user at the time the specific transaction is processed. (CICA, 1998: 219-220)

User identification and authentication generally involve the user presenting one, or a combination, of the following:

- A measure, such as a user name, known to both the parties, with which the user identifies himself/herself,
- Something only the user knows, such as a password, personal identification number (PIN) or a passphrase,
- Something the user has (eg. a smart card, an electronic token or a physical key),
- Something unique about the user based on biometrics (eg. a fingerprint, a hand measurement, a retina scan or a voice recognition measurement). (CICA, 1998: 220)

It is clear that methods for both identification and authentication of a user are necessary before users can be allowed to enter into transactions. “It is increasingly common that, rather than relying on any one single technique, security systems are designed to use a combination of techniques for stronger user identification and authentication.” (CICA, 1998: 220)

The second requirement to address the risk of repudiation is that the processing integrity of the order transaction being sent over the Internet, be ensured by controlling access to the transaction and protect the

information sent over the communication channels from unauthorised access and/or changes.

The general rule of evidence determines that if a person denies a particular signature (which in a manual system proved acknowledgement and acceptance of the transaction), the onus falls upon the relying party to prove that the signature is truly that of the person denying it. The term “deny” is synonymous to the term “repudiate”. This position is supported by standard dictionary definitions. In general terms, the term “non-repudiation” crypto-technically means a service that “provides proof of the integrity and origin of data” (validity) in such a way that it could not be forged or subsequently be refuted. (McCullagh & Caelli, 2000)

According to ISO/IEC 13888-1, -2 and –3 of the International Organisation for Standardisation (ISO), the purpose of non-repudiation in a digital environment is to deliver a services with a aim “to provide verifiable proof or evidence … of”: (McCullagh & Caelli, 2000)

- Approval: proof of whom is responsible for approval of the content of a message,
- Sending: proof of who sent a message,
- Origin: a combination of approval and sending services,
- Submission: proof that a delivery authority has accepted a message for transmission,
- Transport: proof to the originator of the message that a delivery authority has given the message to the intended recipient,
- Receipt: proof that the recipient received the message,
- Knowledge: proof that the recipient recognised the content of a received message, and
- Delivery: a combination of receipt and knowledge services that provides proof that the recipient received and recognised the content of a message.

5 Traditional methods to address repudiation within a digital environment

To enable this legally binding and enforceable “contract” between the buyer and the seller in a digital environment, traditional B2C and B2B systems require that the prospective buyer (customer) provides credit card information, which is immediately, electronically verified with the bank, before transactions entered into via the Internet will be accepted by the seller (supplier). This serves as primary internal control measure to ensure that no orders are accepted and processed by the supplier, before payment for the items could be confirmed.

Within such a system other additional risks, as the provision of stolen credit card information, the intercepting of credit card information, etc., exist which will not be addressed in this report.

According to Williams the following aspects are considered when the validity of traditional contracts is determined: (Williams, 2001)

- Authentication,
- Signature,
- Writing,
- Validity,
- Operational,
- Effective,
- Record, and
- Registered.

In an attempt to determine the validity of a digital contract the abovementioned has to be modified. The following aspects will be considered when a court examines a contract in digital form: (Garcia-Tobar, 2001 and Williams, 2001)

- Authentication that the content of the digital contract is complete and unaltered. Can it be truly verified as the original that the two

parties agreed to? Is there proof that the digital communication involved in the business transaction actually came from the parties that they purport to come?

- Signature: Did the parties involved actually intend to sign the contract and did parties who had the necessary authority within the respective organisations to do so in fact sign the contract? Does the system for the exchange and signing of digital contracts enable each recipient to determine who really sent the message, and whether that individual is in fact who he/she claims to be?
- Writing: both parties signed identical versions of the contract. The contract exists in a standard digital form. Each of the parties, when signing the contract, has submitted their signatures to the other party and was sure of delivery. Does proof exists of the content of the transaction, namely the communications that actually occurred between the parties during the contract formation process?
- Validity: Applicable information, if need be, and so agreed to by the parties, are kept confidential and disclosure of the transaction to unauthorised persons are prevented.
- Operational: The contract was properly time-stamped and it can be verified that the individuals that digitally signed the contract had the authority to sign it at the time they did.
- Record: Both parties can keep a copy of the contract in a tamper-proof and secure manner. Sufficient measures were taken to reduce the possibility of deliberate or inadvertent alteration of the contents of the electronic record of the transaction.
- Registration: If required, the digital contract was recorded at a digital notary service, without indicating where the supplier was located.

It is important to take note from the above that authentication, signing by an authorised part, as well as ensuring the unchanged content of a message (which also contributes to ensuring non-repudiation as

illustrated earlier) are aspects needed to make digital contracts (of which a B2B sales order is one) valid. A valid digital order will thus contribute to prevent repudiation thereof.

6 Open B2B account systems

In addition to the traditional methods of settling e-commerce transactions (by way of credit card payments and verification), “open” B2B accounts emerged. In such systems payment for the transaction does not take place immediately as discussed earlier. In open account systems the purchase is placed on account, to be settled by the customer at a future time, as agreed upon by the two parties – usually at the end of the month by way of an electronic fund transfer (EFT).

The fact that immediate payment for the goods is not ensured, creates an even greater risk for the supplier, namely that payment would never be received - “… while a credit card maximum cap … protects consumers engaging in e-commerce, there are no such guarantees in place for B2B e-commerce” (Garcia-Tobar, 2001). It is therefore even more important to ensure the validity of the digital B2B open account system order before it is accepted and executed.

In 2001 (Morphy, 2001) Amazon wooed its customers with a new credit option - “Amazon Credit Accounts”, which gave consumers the option to pay for their purchases at a later stage, was introduced. Bill Johnson, president of Citi Commerce Solutions, predicted that this new credit option will “create an even better experience” for Amazon.com customers. (Morphy, 2001)

Amazon joined the B2B market by introducing their new “Amazon Corporate Accounts” in 2001. When Amazon first broached the subject of a B2B store, the company said that it anticipated this new sales program to bring in US$150 million over the next two years. Just after launching this initiative Amazon reported that hundreds of organisations, including university libraries, Oracle and 3Com have already signed up for Amazon corporate accounts. (Enos, 2001) This serves to illustrate

the magnitude of the B2B open account e-commerce system.

A prerequisite for such an open account system is the existence of a relationship of trust between the two business partners. To open such an account, a credit application has to be completed and a series of questions be answered to verify the identity of the applicant. If approved, an account number is provided online. To place an order on account, the assigned Amazon credit account number has to be entered as the method of payment on the digital order form. The customer will be billed monthly for all credit purchases made during the preceding period. Customers have the option to pay the entire bill each month or elect to carry a balance on their account. (Amazon.com) Failure to pay the entire bill when it becomes due, will however, lead to interest being charged at high interest rates (Morphy, 2001). Corporate account holders are able to assign account managers and authorised purchasers for their corporate accounts. Account managers will have access to online order history for all account purchases and have the option of receiving notices via e-mail every time a purchase is made (Enos, 2001).

It is thus clear that in a B2B open account system it is essential that internal controls be implemented to specifically:

- Identify and authenticate each other when entering into transactions, especially before accepting and processing these transactions, as well as
- To ensure the processing integrity of these transactions. It must be ensured that, after the initial authorisation of a transaction, no unauthorised changes are made to the content of the transaction.

This will greatly reduce the possibility of a B2B open account order being repudiated by the customer – that is the other supplier in the B2B transaction.

CHAPTER 5

CONTROL OBJECTIVES WITHIN EXISTING CONTROL FRAMEWORKS THAT ADDRESS REPUDIATION

1 Need for control models specifically for IT

While overall business models, like COSO and CoCo (as mentioned earlier) existed, more focussed control models for Information Technology (IT) was necessary. Due to the fact that the available control models was firstly and foremostly frameworks of internal control for management, more detail control objectives that focussed on the need and business objectives for IT specifically, did not exist. With this as aim, the Canadian Institute of Chartered Accountants (CICA) developed “The Information Technology Control Guidelines”.

The Information Technology Control Guidelines defines broad control objectives that is necessary within each area of IT governance (as defined in Chapter 3). It goes further by defining the minimum control standards, including criteria, necessary to meet each defined control objective. Examples of alternative control techniques, or internal control measures, that can be implemented to achieve each of the minimum control standards as defined, are also provided in the Guidelines.

These Information Technology Control Guidelines of CICA evolved and was refined further over the past number of years, as discussed in the following section, to arrive at the two existing control models for IT in particular, namely:

- The Control Objectives for Information and Related Technology (COBIT), and
- The TrustServices Principles and Criteria.

2 Existing control models for IT

2.1 The Control Objectives for Information and related Technology (COBIT)

In an attempt to define clear policies and good practices for security and IT control in particular, the “Control Objectives for Information and related Technology” (COBIT) was developed by The Information Systems Audit and Control Association (ISACA), in 1996 (Weber, 1999: 985). With this the ISACA attempted to be bridge the gaps between business risks, control needs and technical aspects in an IT-environment (COBIT, 2000: 5). Another aim was to bridge the gap between the management models (as COSO) and the more focused control models for IT that existed at this stage (like The Information Technology Control Guidelines of CICA). COBIT aims to be more comprehensive for management and to operate at a higher level than technology standards for information systems management. “Thus, COBIT is the model for IT governance!” (COBIT, 2000: 13). COBIT provides guidance on IT governance by providing the structure that links IT processes, IT resources and information to enterprise strategies and objectives (Hunton, et al., 2004: 3).

According to Romney and Steinbart COBIT is a framework of generally applicable information systems security and control practices for IT control, which focuses on business processes (Romney & Steinbart, 2003: 197 and Weber, 1999: 985). This framework allows:

- Management to benchmark the security and control practices of IT environments,
- Users of IT services to be assured that adequate security and control exists, and
- Auditors to substantiate their opinions on internal control and to advise on IT security and control matters. (Romney & Steinbart, 2003: 197)

In 2000, the COBIT Steering Committee and IT Governance Institute of

ISACA released the third edition of COBIT. It is this edition of COBIT that is used extensively in this report. According to COBIT 3rd edition, adequate control measures need to be defined, implemented and monitored over the IT resources of an organisation (data, application systems, technology, facilities and people) in order to ensure that the business requirements for information (quality-, fiduciary- and security requirements) is met. COBIT breaks down these three requirements into seven distinct categories of information characteristics, namely effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability. (COBIT, 2000: 13-15)

IT managers must achieve these characteristics while balancing the use of their IT resources and it is here where the COBIT Guidelines come in. COBIT designed a framework of IT control objectives for four broad domains, namely organisation and planning, acquisition and implementation, delivery and support and monitoring to assist the managers in this process.

An IT control objective is defined as “a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity” (COBIT, 2000: 12). In order to achieve these IT control objectives, COBIT set out high level control objectives which is then broken up into various specific, detailed control objectives to be achieved.

2.2 TrustServices

AICPA (American Institute of Certified Public Accountants) and CICA are of the opinion, that to be properly effective, the Internet requires a solid foundation of technology, procedures, policies and standards. They acknowledge that human involvement is necessary in the design and implementation thereof. To assist these people in their task the two organisations have, in conjunction, developed and introduced standards to address assurance regarding system reliability and e-commerce activities in particular (AICPA, 2001). These standards consisted of

"Principles and Criteria" and were specifically applicable to two AICPA/CICA services, namely SysTrust (for any defined electronic system) and WebTrust (which specifically addressed electronic commerce).

AICPA and CICA have since began harmonising the underlying "Principles and Criteria" by developing the "Trust Services Principles and Criteria". It is currently issued in draft form under a common banner of "Trust Services". The two bodies do not intend to change SysTrust or WebTrust services, or to introduce additional branded services at this stage. Both SysTrust and WebTrust products and services remain unchanged at this point in time as assurance and advisory services.

The effective date for the application of the Trust Services Principles and Criteria is for appointments commencing on/after 1 April 2003 (AICPA, 2003). Due to the fact that the TrustServices Principles and Criteria supersedes the existing SysTrust Principles and Criteria version 2.0 and version 3.0 of the WebTrust Principles and Criteria, it will be used in this study.

TrustServices specifically focuses on internal control and, after being submitted to an examination, an opinion is expressed indicating whether a specific website met the requirements of the "TrustServices Principles and Criteria". This certification is displayed on the website concerned and certifies that the website maintains the necessary controls in 5 areas, namely:

- Online Privacy,
- Security,
- Confidentiality,
- Availability, and
- Processing Integrity.

With this process the experience and reputation of respected e-commerce experts and advisors worldwide can be utilised to assist the supplier in identifying business risks, as well as making

recommendations for the necessary controls that could be implemented to address the risks identified. For consumers and visitors to a website which bears the certificate concerned, this independent seal means reliability, which also contributes to attracting and keeping good customers. A licensed Certified Public Accountant (CPA), Chartered Accountant (CA), or other equivalent provides this certificate after performing the examination required. The websites are periodically reviewed to ensure compliance with the latest principles.

3 Control objectives and principles from existing control models that address repudiation

As mentioned previously, both COBIT and AICPA and CICA's TrustServices defines control objectives and/or principles applicable to IT systems and e-commerce systems in particular. The control objectives and/or principles from each of the respective models that address repudiation are discussed in the following paragraphs.

3.1 Control objectives from COBIT

One of the control objectives formulated by COBIT is to "Ensure Systems Security" (DS5) (COBIT, 2000: 101). This is defined as "Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorised use, disclosure or modification, damage or loss, and is enabled by logical access controls which ensure that access to systems, data and programmes is restricted to authorised users and takes into consideration … authorisation, authentication and access control, user identification and authorisation profiles …" (COBIT, 2000: 100). It should be clear from this definition that ensuring system security will contribute towards ensuring non-repudiation of transactions.

The following detailed control objectives which assist to "Ensure Systems Security", is regarded as applicable to address the particular

risks as illustrated in this report: (COBIT, 2000)

- Identification, Authentication and Access (DS5 – 5.2),
- Transaction Authorisation (DS5 – 5.14),
- Non-Repudiation (DS5 – 5.15), and
- Trusted Path (DS5 – 5.16).

These detailed control objectives and their contribution to address the topic of this report is discussed below.

3.1.1 Identification, Authentication and Access

COBIT's detailed control objective Identification, Authentication and Access is defined as follows:

"The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorised personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimise the need for authorised users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective" (COBIT, 2000: 101).

This control objective thus necessitates the implementation and maintenance of appropriate identification-, authentication- and authorisation mechanisms, including clear access rules, in order to limit access to the system, the data and other IT resources. If implemented, this will contribute to prevent unauthorised persons for gaining access to a supplier's system to place unauthorised orders on the accounts of valid B2B open account system customers. It will also prevent unauthorised changes to previously approved transactions by limiting access.

3.1.2 Transaction Authorisation

To achieve the detailed control objective Transaction Authorisation, the "Organisational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system" (COBIT, 2000: 102).

This entails that, in an attempt to properly authorise a transaction, it is critical to authenticate the transaction as well as the identity of a potential customer. This will contribute to prevent unauthorised persons from entering into unauthorised transactions on the open accounts of valid B2B customers.

3.1.3 Non-repudiation

According to COBIT, an organisation policy that ensures that, where appropriate, neither party can deny transactions, as well as controls implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions, are essential fundamentals to provide non-repudiation services. (COBIT, 2000: 103)

COBIT thus specifically requires that to ensure system security the necessary internal control measures should be implemented to ensure non-repudiation.

3.1.4 Trusted Path

A Trusted Path must exist and be maintained between the two parties to a transaction. According to COBIT "organisational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys" (COBIT, 2000: 103). It would contribute to reduce the possibility of messages being intercepted and/or unauthorised changes being made to it during transmission, resulting in customers repudiating order transactions.

3.2 Principles from Trust Services

The two TrustServices' principles that relates to the risks addressed in this report, are:

- Security, and
- Processing Integrity.

3.2.1 Security

According to TrustServices, the Security-principle refers to "the protection of the system components from unauthorised access, both physical and logical. In e-commerce … systems, the respective parties wish to ensure that information provided is available only to those individuals who need access to complete the transaction … Limiting access to the system components helps prevent potential abuse of system components, … improper access to, (and) use (of) …" (AICPA, 2003: 5). The risks that form the purpose of this study are therefore partly addressed under this principle.

Under this principle, specific criteria that will assist in achieving this objective, is described. Applicable criteria under Security that will address repudiation, is: (AICPA, 2003)

"3.1 Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters:

b. Identification and authentication of users.

…

d. The process to grant system access privileges and permissions.

3.3 Procedures exist to protect against unauthorised logical access to the defined system.

…

3.5 Encryption or other equivalent security techniques are used to

protect user authentication information and the corresponding session transmitted over the Internet or other public networks." (AICPA, 2003)

3.2.2 Processing Integrity

Processing Integrity is defined in TrustServices as follows: "The processing integrity principle refers to the completeness, accuracy and timeliness, and authorisation of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorised or inadvertent manipulation" (AICPA, 2003: 25).

It is under the "authorisation"-part of the Processing Integrity-principle that the risk of unauthorised changes to previously authorised transactions is addressed. Authorisation includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing (AICPA, 2003). It is important to note that "If a system processes information inputs from sources outside of the system's boundaries, an entity can establish only limited controls over the … authorisation … of the information submitted for processing" (AICPA), as is the case with order transactions (input) handled by e-commerce systems where data is directly entered via Web-enabled input screens or forms by the users.

Specific criteria within Trust Services under the Processing Integrity-principle that addresses the risk of unauthorised changes in particular, is: (AICPA, 2003)

"3.1 The procedures related to … authorisation of inputs are consistent with the documented system processing integrity policies.

If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters:

…

- Positive acknowledgement is received from the customer

before the transaction is processed.

…

3.4 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

b. Identification and authentication of users.

…

d. The process to grant system access privileges and permissions.

…

3.7 Procedures exist to protect against unauthorised logical access to the defined system.

3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks." (AICPA, 2003)

CHAPTER 6

INTERNAL CONTROL MEASURES FOR NON-REPUDIATION

1 Internal control measures recommended by existing control models

In the preceding chapter it was shown that both COBIT and the TrustServices Principles and Criteria have defined particular objectives or principles that address the risks that form the basis of this report. It was also mentioned that both institutions provides examples of recommended internal control measures that can be implemented to address the objectives as defined. In this chapter these internal control measured are identified.

2 Recommendations by COBIT

According to COBIT, procedures such as regular changes to passwords should be in place to keep authentication and access control mechanisms effective. This will among others ensure proper Identification, Authentication and Access as defined (COBIT, 2000: 101).

Transaction authorisation requires the use of cryptographic techniques for signing and verifying transactions, to determine the authenticity of a transaction and the validity of the user's claimed identity (COBIT, 2000: 102).

Techniques which can be implemented to achieve the control objective Non-Repudiation includes the use of digital signatures, time stamping and trusted third parties, with appropriate policies that take into account relevant regulatory requirements (COBIT, 2000: 103).

To establish a Trusted Path it may, according to COBIT, necessitate the use of encryption between users, between users and systems, and

between systems (COBIT, 2000: 103).

3 Recommendations by TrustServices

3.1 Security

The following internal control measures, that are included in the TrustServices Principles and Criteria's Security-principle, can be utilised to address the risks identified in this report: (AICPA, 2003)

- Unique user ID's are assigned to individual users. Users are required to log on to the entity's network and application systems with their user ID's and password before access is granted. Sound password control include passwords to contain at least six characters, one of which is non-alphanumeric, passwords being case sensitive and passwords to be updated every 90 days.
- All paths that allow access to significant information resources (access paths) are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles.
- The ability to create or modify users and user access privileges is limited to the security administration team alone.
- The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator.
- Virtual private networking (VPN) software is used to permit remote access by authorised users. The VPN server through specific "client" software, as well as user ID and passwords authenticates users.

  A virtual private network is a network that controls access to an extranet by encryption and authentication technology. With this technique the functionality of a privately owned network is provided,

whilst the Internet, a worldwide network, is being used (Romney & Steinbart, 2003: 66).

- Unneeded network services are deactivated on the entity's servers.
- Firewalls are used and configured to prevent unauthorised access. Firewall events are logged and reviewed daily by the security administrator.

  A firewall consists of a "combination of security algorithms and router communication protocols that prevent outsiders from tapping into corporate databases and e-mail systems." This technique prevents unauthorised access by both outside parties, as well as employees, who attempt to gain access to parts of the system they should not have access. It provides "a barrier between the networks that prevents unwanted information from flowing into and out of the trusted network (Romney & Steinbart, 2003: 245).
- Intrusion detection systems provide continuous monitoring of the entity's network and early identification of potential security breaches.
- The organisation contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
- The organisation uses 128-bit secure sockets layer (SSL) encryption for transmission of … information over public networks, including user ID's and passwords.
- Account activity, subsequent to successful login, is encrypted through a 128-bit secure sockets layer (SSL) session.
- Users are logged out on request, or after 10 minutes of inactivity.

3.2 Processing Integrity

According to the TrustServices Principles and Criteria, the following controls under Processing Integrity will, additionally to those mentioned

in the preceding section, prevent unauthorised access to, and changes to information during transmission (AICPA, 2003):

- Logical access controls such as user identification and authentication systems, passwords, physical possession or biometric identification, etc.
- Customer account manager performs regular reviews of customer complaints, back-order logs, and other transactional analysis. This information is compared to customer service agreements.
- During transmission information is protecting using a variety of methods including:
  - Encryption of transmission information.
  - Batch header and control total reconciliations.
  - Message authentication codes and hash totals.
  - Private leased lines or virtual private networking connections with authorised users.
  - Bonded couriers and tamper-resistant packaging.
- The entity e-mails an order confirmation to the customer-supplied e-mail address. The order confirmation contains, among others, order details as well as shipping and delivery information. Returned e-mails are investigated by customer service.
- Input transactions are date and time stamped by the system and identified with the submitting source (user, terminal, IP address).
- Each order has a unique identifier that can be used to access the order and related shipment and payment settlement information.

4 Additional control measure that will address the repudiation risk

Additionally to the controls as recommended by COBIT and TrustServices, there are other important aspects to consider when

receiving orders placed on open accounts in B2B systems. Garcia-Tobar divides these controls into two basic categories, namely:

- Operational procedures, and
- Technology choices or concerns (Garcia-Tobar, 2001).

4.1 Operational procedures

- Companies should retain and hire personnel that are familiar with security operation procedures and have personal knowledge of how a system can operate securely, and how it actually operated during creation or storage of a record. Alternatively, they should outsource this function to a dedicated provider of trust and security systems.
- Trust provider systems (software components specifically geared towards providing trust and security requirements) should be supported (or purchased) from vendors that support trusted software engineering processes that leave a trail of design decisions for each stage in the manufacturing process. The trail support proves the reliability of a records system, which in turn supports the claim of integrity, authenticity, and admissibility of a record as evidence. The functions and systems of trust provider's system should be documented in a formal "security target" documentation format.
- E-business applications specifically targeted at trust and security should be subjected to periodic security audits according to criteria laid down either by the state licensing authorities or by mutual consent of the parties. These checks should measure the effectiveness of the management, operational and technical controls of all trustworthy systems.
- Companies must validate the identification credentials presented to them. Without validation fraudulently obtained or revoked digital certificates can be used to access confidential information or

infiltrate the heart of a business.

- Organisations must have a secure, fast and reliable way to send sensitive data over Internet.
- Companies must be able to securely generate, exchange, archive and reconstruct e-transactions in an auditable manner.
- Electronic contracts and transactions must be made legally binding by providing all essential elements of non-repudiation.
- Digital receipts, that offer proof that an e-transaction occurred at a specific time and date must be used. (Garcia-Tobar, 2001)

4.2 Technology choices

- Use digital signature technology and certificate authorities. Fundamentally, electronic commerce involves the use of remote communications and therefore necessitates all parties involved to authenticate one another. One of the primary technologies proposed for authentication is digital signature technology.

  A further claimed advantage of digital signature technology concerns the issue of 'non-repudiation' claimed by the relying party against the 'alleged' signer of an electronic document (McCullagh & Caelli, 2000).

  Certificate authority (CA) can be chosen by determining the use of digital signatures for authenticating the identity of individuals involved in business transactions. Validation can be achieved by building a set of e-business applications in such a way that all digital certificate transactions and digital signatures are validated in real-time prior to acceptance (Garcia-Tobar, 2001).

  A digital signature is an electronic message that uniquely identifies the sender of the message, similarly to the way in which a handwritten signature uniquely identifies the person signing a paper document. It is achieved through public key infrastructure (PKI), a

method of encryption using two sets of keys. The own key, the “public key” is publicly available, whilst the second key, the “private key”, is kept secret and is only known to the owner of the two particular keys. Any one of the two keys (“public” or “private”) can be used to encrypt a message, whilst only the other key of the particular “public-private”-pair can be used to decode the message.

A digital certificate identities the owner of a particular “private key” and the corresponding “public key”, as well as the time during which the certificate is valid. These digital certificates are issued by reliable third parties, known as “certificate authorities”. Verisign, Entrust and Digital Signature Trust are examples of well-known certificate authorities. (Romney & Steinbart, 2003: 62)

- Secure delivery and receipt transactions, authenticated using trusted infrastructure services must be properly ‘received’. The recipient should formally acknowledge error-free delivery of data and also formally accept responsibility for handling of the transaction.
- All business applications should be acknowledged with a tamperproof digital receipt that can be stored in a long-term, secure and tamper-proof way.
- Enterprises should retain records of transactions and contracts, along with digital certificates for pre-specified records and retentions periods. (Garcia-Tobar, 2001)

CHAPTER 7

MATRIX OF NON-REPUDIATION OBJECTIVES AND APPROPRIATE INTERNAL CONTROL MEASURES

Taking into account the information as set out in the previous chapters, the following are the most important objectives to ensure non-repudiation of a specific B2B order transactions within an open account system:

- **Identification** of the prospective customer/user.
- **Authentication** of the user before entering into a transaction.
- An identified and authenticated user is only granted access to the system according to the pre-defined authorisation rules – this implies **limiting access,** whilst ensuring that adequate division of duties is enforced as well.
- All attempts to gain unauthorised access or to make unauthorised changes are identified, logged and followed-up – adequate **monitoring.**
- The **integrity** of a transaction transmitted over the communication channel is guaranteed to ensure that no unauthorised changes are made to previously authorised transactions.

As set out in Chapter 6, there are various techniques or internal control measures that can be implemented to achieve the above-mentioned objectives or to address the risks as defined for a supplier receiving an order in a B2B open account system.

The objectives as defined above, as well as the main categories of internal control measures (as per Chapter 6) that can be implemented to achieve them, is presented in the matrix that follows.

	OBJECTIVES				
TECHNIQUES	**Identification**	**Authentication**	**Limiting Access**	**Monitoring**	**Integrity**
• Competent, reliable employees are in control of system security, or this services is outsourced to a reliable supplier of security services			X		X
• User profiles are defined	X				
• Users log on using unique user ID's and passwords	X				
• Adequate control over passwords	X				
• Access is only granted to authenticated users according to the defined user profiles		X	X		X
• All access routes to the system are controlled, using access control systems and/or operating systems	X		X		X
• Users are logged-out on request, or after 10 minutes of non-activity on the system	X				
• Control over the creation and amendment of passwords and user profiles	X				
• Log-on sessions are terminated after 3 unsuccessful attempts to gain access	X				

	OBJECTIVES				
TECHNIQUES	**Identification**	**Authentication**	**Limiting Access**	**Monitoring**	**Integrity**
• Unsuccessful attempts to gain access are recorded and followed-up				X	
• Cryptographic techniques are used to sign and verify transactions		X			
• All parties involved identify and authenticate one another before access is granted – by for example making use of digital signature technology with PKI		X			
• Trusted third party certificate authorities, for example Verisign, Entrust and Digital Signature Trust, are used		X			
• Provide input transactions with date- and time stamping which can be verified by the source (user, terminal, IP address)		X			X
• Digital acknowledgements of receipt, with the specific date and time of transaction is provided	X	X			X
• Computer activity and messages (including userID's and passwords) transmitted between users, between					

	OBJECTIVES				
TECHNIQUES	**Identification**	**Authentication**	**Limiting Access**	**Monitoring**	**Integrity**
users and systems, as well as between systems, are protected by using among others: - Encryption of information, using a 128-bit secure sockets layer (SSL) session - Batch header and control total reconciliations - Message authentication codes and hash totals - Privately leased lines, or virtual private networks with authorised users - Bonded couriers and tamper-resistant packaging					X
• Virtual private network (VPN) software is used to authenticate outside users and control their access to the system		X			X
• Firewalls are configured to control all access to the system • Firewall-activities are recorded and reviewed daily			X X		

	OBJECTIVES				
TECHNIQUES	**Identification**	**Authentication**	**Limiting Access**	**Monitoring**	**Integrity**
• All possible security breaches are followed up			X		
• Intrusion detection systems are used to monitor the system continuously • All possible security breaches are followed up				X X	
• Independent third parties perform periodic reviews of system security and control. Results and recommendations are reported to management directly	X	X	X	X	X
• E-business security software are subjected to periodic security audits, that evaluates management-, operating-, as well as technical controls	X	X	X	X	X

CHAPTER 8

SUMMARY AND CONCLUSION

The statement of the problem to be addressed in this report as well as the purpose of this study, the methodology applied, as well as the limitations of the study was provided in Chapter 1.

The concept of business risk, the purpose of internal control and various control frameworks for internal control was defined and illustrated in Chapter 2. It was mentioned that business risks are created as transactions take place between business partners. These risks differ within each industry as well as within each business cycle. Various internal control measures can be implemented to address business risks associated with transactions. To design an adequate system of internal control, risk management has to be applied.

A sales transaction taking place between two business partners was chosen to form the topic for further study in this report. It was illustrated that one of the most important risks a supplier faces when selling physical items to a customer is the risk of repudiation of the transaction by the customer. This leads to the supplier suffering financial losses.

The reasons for repudiation was investigated and in Chapter 3 it was found to be the result of one of two possible situations, namely:

- Unauthorised orders placed on behalf of an existing customer, and/or
- Subsequent unauthorised changes made to previously authorised order transactions.

To ensure non-repudiation a supplier therefore needs to implement the necessary internal control measures to address the particular risk. The relevant controls that can be implemented by a supplier to address repudiation within a manual system were mentioned in Chapter 3.

The sales transaction process was “translated” to a computer environment and it was illustrated in Chapter 3 that the principles of risk and internal control measures are still applicable when a supplier operates within a computerised environment. The importance of IT – governance, namely to ensure that the necessary internal control measures are implemented within an IT environment, was mentioned. Examples of the internal control measures that could be implemented by a supplier to ensure non-repudiation within a computerised environment was provided in Chapter 3.

In Chapter 4 the Internet, e-business, e-commerce, B2B commerce and open B2B account systems was defined. The significance of B2B transactions, which forms the topic of this report, was illustrated.

E-business risk and the fundamental problems that arise when conducting e-business transactions were mentioned. The objectives of ensuring non-repudiation in a digital environment were illustrated. The traditional methods to enable a legally binding and enforceable contract between a supplier and customer were illustrated.

The problems and risks that a supplier, who provide for customers buying on open B2B accounts, faces were illustrated in Chapter 4. It was deducted that a prerequisite for such an open account system is the existence of a relationship of trust between the two business partners. The B2B business partners need to ensure that the necessary internal control measures are implemented to specifically:

- Identify and authenticate each other when entering into transactions, especially before accepting and processing transactions, as well as
- To ensure the processing integrity of these transactions. It must be ensured that, after the initial authorisation of a transaction, no unauthorised changes are made to the content of the transaction.

In Chapter 5 the two existing control models for IT were identified. They are:

- The Control Objectives for Information and related Technology (COBIT) of ISACA, and
- The TrustServices Principles and Criteria, a joint initiative of AICPA and CICA.

It was found that the following detailed control objectives as defined by COBIT will assist to Ensure Systems Security and was regarded as applicable to address the particular risks as illustrated in this report:

- Identification, Authentication and Access,
- Transaction Authorisation,
- Non-Repudiation, and
- Trusted Path.

The two TrustServices' principles that relates to the risks addressed in this report, are:

- Security, and
- Processing Integrity.

The internal control measures recommended by COBIT and TrustServices to assist in providing non-repudiation services was identified and listed in Chapter 6. Additionally to these, it was found that there are operational procedures, as well as technology choices that would contribute in ensuring non-repudiation for B2B open account system suppliers. These were also briefly mentioned in Chapter 6.

Based on the study performed the most important objectives to prevent the repudiation of a specific B2B order transaction within an open account system were formulated. They are:

- Identification of the prospective customer/user,
- Authentication of the user before entering into a transaction,
- An identified and authenticated user is only granted access to the

system according to the pre-defined authorisation rules – this implies limiting access whilst ensuring that adequate segregation of duties is enforced as well,

- All attempts to gain unauthorised access or to make unauthorised changes is identified, logged and followed-up – adequate monitoring, and
- The integrity of a transaction transmitted over the communication channel is ensured – no unauthorised changes are made to previously authorised transactions.

In Chapter 7 the way in which the internal control measures identified in Chapter 6 would ensure that each of the objectives defined above could be achieved, were illustrated by way of a matrix.

The purpose of this study as defined in Chapter 1, namely a framework of internal control measures that can be implemented by B2B suppliers to address the risk of repudiation when orders are placed on open accounts are received, was thus achieved.

If the control measures contained in the framework are implemented by the B2B suppliers concerned it would lead to an improved system of internal control. It will decrease the occurrence of repudiation due to invalid orders that were accepted and processed, or processed whilst containing unauthorised changes. These controls should thus lead to the prevention or reduction of losses suffered by B2B suppliers as a result of repudiation.

LIST OF ACRONYMS

AICPA – American Institute of Certified Public Accountants

CICA – The Canadian Institute of Chartered Accountants

COBIT – Control Objectives for Information and related Technology

COSO – Committee of Sponsoring Organisations

ISACA – The Information Systems Audit and Control Association

SAICA – South African Institute of Chartered Accountants

REFERENCES

AICPA 2001

Online Business - E-commerce Today – Risks and Rewards

http://www.webtrust.org/online.htm - accessed on 19 June 2003

AICPA 2003

Suitable TrustServices Criteria and Illustrations, effective for engagements beginning on or after April 1, 2003 - Website http://www.aicpa.org/assurance/trustservices

AICPA websites visited

http://www.aicpa.org/assurance/trustservices
http://www.aicpa.org/assurance/systrust.princip.htm
http://www.aicpa.org/trustservices/ecommentnewsletterpa1102.htm

Amazon

http://www.amazon.com - accessed on 21 July 2003

Arens Alvin A, Loebbecke James K, 2000

Auditing an Integrated Approach, 8th edition, Prentice Hall International, 2000

Bartlett Micheal, 2000

B2B Purchasing Will Double By 2002, 28 November 2000

http://www.findarticles.com/cf_dls/m0NEW/2000_Nov_28/67385197/p1/article.jhtml?term=B2B%2B%22open+account%22

Bartlett Micheal, 2001

CEOs Foresee Glowing Future for Internet E-Commerce, 6 December 2001, University of Stellenbosch – Computer Database, Article A80641161

Boynton William C, Johnson Raymond N, Kell Walter G, 2001

Modern Auditing, 7th edition, John Wiley & Sons, Inc, 2001

CICA, 1998

Information Technology Control Guidelines, 3rd edition, The Canadian Institute of Chartered Accountants, 1998

COBIT, 2000

Control Objectives for Information and related Technology (COBIT), 3rd edition, July 2000

http://www.isaca.org/cobit.htm

Electronic Communications and Transactions Bill

Enos Lori, 2001

Amazon extents credit to corporate buyers, E-Commerce Times, 22 Augustus 2001

Garcia-Tobar Alex, 2001

Legalising B2B e-commerce, March 2001

Gartner

http://www.gartner.com

http://searchcio.techtarget.com - accessed on 3 June 2003

Hunton James E, Bryant Stephanie M, Bagranoff Nancy A, 2004

Core concepts of Information Technology Auditing, 1st edition, John Wiley & Sons, Inc, 2004

King Report, 2002

The second King Report on Corporate Governance in South Africa, issued by the Institute of Directors, effective from 1 March 2002

KPMG, 2001

KPMG Enterprise Risk Management Services

http://www.kpmg.com/Rut2000_prod/Documents/9/ERM.pdf

Mc Cullagh Adrian, Caelli William, 2000

Non-repudiation in the digital environment, First Monday, Volume 5, number 8, August 2000 - http://firstmonday.org/issues

Morphy Erika, 2001

Amazon woos customers with new credit option, ECT News Network, 5 November 2001

Moscove Stephen A, 2001

E-Business Security and Controls, CPA Journal, 07328435, November 2001, Volume 71, Issue 11 - University of Stellenbosch - Business Source Premier Database, accessed on 21 July 2003

Naidoo Samesh, 2002

Managing risk and organisational performance, Accountancy SA, August 2002

http://www.accountancysa.com - accessed on 14 October 2003

Protiviti, 2003

Enterprise business risk management process – Overview, Internal Audit and Risk management Community

http://www/protiviticonsulting.com/aboutus/index.html - accessed on 21 July 2003

Romney Marshall B, Steinbart Paul John, 2003

Accounting Information Systems, 9th edition, Prentice Hall, 2003

SAICA

SAAS 400, Risk assessment and Internal control, South African Institute of Chartered Accountant (SAICA)

Sairamesh J, Mohan R, Kumar M, Hasson L, Bender C, 2002

A platform for business-to-business sell-side, private exchanges and marketplaces IBM Systems Journal, July 2002, Volume 41, Issue 2, p 242 (11), University of Stellenbosch – Computer Database

Stallings William, 1995

Network and Internetwork Security – Principles and Practice, Prentice Hall, IEEE Press, 1995

Unknown author, 2000

B2B Marketplaces Rapidly Transforming World Economy, 1 February 2000

http://www.findarticles.com/cf_dls/m4PRN/2000_Feb_1/59108161/p1/article.jhtml?term=B2B%2B%22open+accounts%22

Wagner Bill, 2000

Preparing for the E-generation, March 2000, Volume 4, Issue 3, p18, University of Stellenbosch - Computer database - HP Professional

Ward Lynn, 2003

The New face of B2B E-Commerce, E-Commerce Times, 22 May 2003 - http://www.ecommercetimes.com – accessed on 21 July 2003

Weber, 1999

Information Systems Control and Audit, The University of Queensland, Prentice Hall, 1999

Webtrust website

http://www.webtrust.org

Williams ART, Dale BG, Visser RL, Van der Wiele T, 2001

B2B, old economy businesses and the role of quality – part 1 – the simple alternative, Measuring Business Excellence, Volume 5, number 2, 2001, pp 39-44

Williams Peter, 2001

Security: securing legal-grade transactions on the Web digital signatures & validation. The future of high value EDT, Software World, September 2001, Volume 32, Issue 5, p 18(2) – University of Stellenbosch Computer Database - Thomson Gale Article A93211193