B2B suppliers: Addressing the repudiation of orders in an open account system

R Butler

Department of Accountancy
University of Stellenbosch

Abstract

Suppliers suffer losses when customers repudiate B2B order transactions in open account systems. Appropriate internal control measures should be implemented to address repudiation. According to the King Report on Corporate Governance for South Africa (2002), the responsibility for internal control lies with the management of a company.

This article aims to assist management in reducing the risk of repudiation to an acceptable level, by providing a framework of recommended internal control measures. The framework was compiled after considering:

Requirements in the Electronic Communications and Transactions Act that make digital contracts valid.

Existing control frameworks, control objectives and internal control measures addressed by COBIT® and AICPA/CICA's Trust Services Principles and Criteria.

Key words

B2B
Non-repudiation
e-commerce
Internal control
Repudiation
e-business
Risk

"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 and Steinbart 2003:61)

1 Introduction

In a computerised system, non-repudiation forms one of the five categories of Information Security Goals, as defined by the International Organisation for Standardisation (ISO) (Tak, Lee and Park 2003; Hartman 2003:5; Zhou and

Gollmann 1997). Non-repudiation is also an essential feature in establishing the legal basis of an electronic transaction (Tak *et al* 2003).

The repudiation of order transactions by customers is a major business risk faced by almost all suppliers (Laudon and Traver 2004:318). This is particularly true of business-to-business (B2B) suppliers, when customers are allowed to place orders on open accounts. The reason for this is that in B2B open account systems, the payment for a transaction concluded via the Internet does not take place immediately. Instead, purchases are placed on accounts that accumulate, to be settled at a future date.

B2B suppliers who have already manufactured, packaged, transported and delivered goods suffer monetary losses when customers subsequently repudiate these B2B orders placed on open accounts. According to Laudon and Traver (2004:318), the costs for suppliers when customers repudiate transactions can be significant: ". . . roughly 3.5% of the purchase plus a transaction fee of 20-30 cents per transaction, plus other set-up fees". To minimise such losses and reduce this risk to an acceptable level, an effective system of internal control has to be implemented.

The Information Systems Audit and Control Association (ISACA) is of the opinion that, when computer systems are involved, it is critically important for the survival and success of an organisation to manage information and the related information technology (IT) effectively. 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).

According to the King Report on Corporate Governance, the responsibility for assessing risk exposure (including operational and technology risks) and to design, implement and maintain a comprehensive system of internal control to address the risks a company is exposed to (referred to as the risk management process), lies with the management of a company (King Report on Corporate Governance for South Africa 2002: Section 1, paragraph 3).

As the environment in which a business operates and/or the technology utilised in the business process change, the "methods" used to address the risks (that is the internal control measures that can be implemented) change (Romney and Steinbart 2003:61). According to King, responsible management needs to demonstrate adequate knowledge of modern IT-enabled systems, as well as an appreciation of the related changes in the organisation's internal control system in an information technology (IT) environment (King Report on Corporate Governance for South Africa 2002: Section 5, Chapter 4). Internal control measures have to be "adopted and adapted to fit in with a computer environment" (Weber 1999:13). The internal control measures that address repudiation in a manual system would clearly have to be adapted in a computerised environment to still address the risk of repudiation sufficiently.

It is thus essential that the management of B2B suppliers implement a suitable system of internal control measures to address the particular risk of repudiation of B2B orders placed on open accounts by customers. The purpose of this article is to assist management in this task by providing a framework of recommended internal control measures that can be implemented to reduce this risk to an acceptable level. This framework is contained in Table 1.

Implementing these internal control measures will contribute to minimising the losses suffered by suppliers as a result of repudiation, as well as assist management in fulfilling its responsibility with regard to internal control measures to ensure non-repudiation.

2 Research method and scope

2.1 *Research method*

To develop this framework of recommended internal control measures, this article is structured as follows:

1 Discussion of risk and the need for a system of internal control (Section 3).

   The first step in the risk management process is for management to identify the key risk areas within the company. One of these risks, namely repudiation, forms the subject of this article.

2 Explanation of repudiation and identification of the reasons why the repudiation of orders by customers occurs (Section 4).

   Before management can design and implement internal control measures to address the problem, management must first grasp the meaning of repudiation and understand the purpose of non-repudiation services. To be able to address the problem adequately, it is essential that management be familiar with the reasons why orders are repudiated by customers and understand when and where the problem originated.

   Applicable sources and definitions were studied and the meaning of repudiation was determined and analysed. Based on what repudiation entails, the two major reasons why customers typically repudiate order transactions were deduced.

3 Illustration of how repudiation can be addressed within a **manual system** (Section 5).

   The risk of repudiation also exists within a manual system. The internal control measures that ensure non-repudiation within a manual ordering system would be insufficient to address the problem in a B2B environment. Hence, the internal control measures aimed at ensuring non-repudiation within a manual ordering system are highlighted in order to arrive at a set of basic objectives that need to be achieved by the internal control system in a computerised environment in order to ensure non-repudiation.

4 Investigation and definition of the **digital environment** and **B2B open account systems** (Section 6). Illustration of how **non-repudiation in a digital environment** is ensured (Section 7).

The information gathered in Steps 1 to 3 is 'translated' to the B2B environment. Typical internal control measures that are available to address repudiation in a computerised system are explained.

5 Determination of the **aspects** that are required **to make B2B sales orders legally binding** (Section 8).

In order to prevent an order placed in the digital environment from being repudiated, it is necessary for the order to be declared valid and thus to be made legally binding – it must be deemed a 'digital contract' which cannot be denied.

The Electronic Communications and Transactions Act, which regulates digital communications and transactions, was studied to determine which aspects would be considered when assessing the evidential weight of data messages. If B2B orders placed in open account systems were to meet the requirements to make a digital contract (the order) valid, subsequent repudiation of the order would be prevented.

6 Formulation of the most important objectives to ensure non-repudiation and identification of the relevant internal control measures that can be implemented to achieve these objectives (Section 9).

The information contained in the documentation of the IT-governing bodies, namely the *Control Objectives for Information and Related Technology* (COBIT®) and the *Trust Services Principles and Criteria* (a joined effort by The Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA)) were studied. These bodies focus on IT and their documentation should be considered in the process of IT governance.

Taking into account the control objectives and/or principles as defined in COBIT®, and the *Trust Services Principles and Criteria*, the most important objectives to ensure the non-repudiation of a specific B2B order transaction within an open account system are formulated.

Finally, by taking into account the internal control measures laid down by the aforementioned IT-governing bodies, the main categories of relevant internal control measures necessary to achieve the formulated objectives and thus address the repudiation of these orders in a B2B environment, are identified.

These recommended internal control measures are linked to the objectives to be achieved to ensure non-repudiation and they are set out in a matrix contained in Table 1.

2.2 *Scope*

It is important to note that this article only addresses the repudiation problem from the perspective of a B2B supplier, and that it only focuses on those problems relating to orders for physical products. Although some of the related concepts and risks may be present in the environment that forms the topic of this article, Internet sales of digital and electronic products (such as ShareWare), as well as the provision of services, fall beyond the scope of this article.

This study is also limited to B2B open account systems. The traditional settling of e-business transactions by means of credit cards, where the creditworthiness of the customer and payment for the goods are immediately electronically verified by the supplier, do not form part of this study.

Lastly, this article does not intend to address the technical issues regarding the functioning of any of the internal control measures recommended, but merely to provide a framework for the appropriate internal control measures.

3 Risk and internal control

When any transaction takes place between two business partners, risks are created as soon as rights and obligations change hands. According to the King Report on Corporate Governance, risks are "uncertain future events that could influence the achievement of a company's objectives" (King Report on Corporate Governance for South Africa 2002: Section 2, Chapter 1). CICA's *Information Technology Control Guidelines* (1998:409) defines a risk as any process, activity or event that can negatively influence the successful, sustainable and ethical achievement of enterprise objectives.

Business risk is "the likelihood that an organisation will not achieve its business goals and objectives" (Hunton, Bryant and Bagranoff 2004:48). A particular risk exists as a result of the location or method of operation of a particular function (*Information Technology and Control Guidelines* 1998:8). Risk varies according to the circumstances in which a company finds itself. Both internal and external factors may contribute to the possibility that a risk will occur (Hunton *et al* 2004:48). The risks faced by a company are also influenced by the industry within which the company operates, and new risks are introduced as companies change their business processes and models.

To address the business risks present within any transaction cycle, the necessary internal control measures, or a so-called system of internal control, should be implemented. The Committee of Sponsoring Organisations of the Treadway Commission's report *Internal Control – Integrated Framework* (COSO 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 . . . ". *The Information Technology and Control Guidelines* (1998:11) 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.

It is evident from the COSO report (1992), and the notion is supported by the King Report on Corporate Governance for South Africa (2002: Section 1, paragraph 3), that the directors of a company are responsible for the total process of risk management, which includes identifying the key risk areas, designing and implementing internal control measures, monitoring the process of risk management and integrating it into the day-to-day activities of a company.

A typical sales transaction holds numerous risks for both the buyer (customer) and the seller (supplier). When a sales transaction takes place, the supplier (seller) incurs costs to manufacture, package and deliver the goods as soon as a sales order is approved and accepted. On delivery of the goods, the customer (buyer) is responsible for paying the supplier the monetary value or cost of the items delivered.

One of the major business risks that a sales transaction poses to the supplier is the risk of repudiation of the order by the customer. The risk of repudiation increases substantially in systems in which goods are sold to customers on credit. "With cash, purchases tend to be final and irreversible (i.e., they are irrefutable) unless otherwise agreed by the seller" (Laudon and Traver 2004:309). In a credit system, payment for the items does not take place immediately on delivery of the items, but at some future date as agreed upon by the parties involved, thereby increasing the risk that the supplier may suffer monetary losses if transactions are repudiated.

The main reason for choosing the repudiation of order transactions by customers as the topic of study is the fact that repudiation is a specific risk within any sales cycle and particularly so in a B2B open account system, as illustrated in this article. If repudiation occurs, it has financial implications for businesses (suppliers) that have invested time, resources and effort in fulfilling the order.

If management can prevent repudiation, management will minimise the losses suffered as a result of repudiation. In order for management to be able to achieve this, it first has to understand what repudiation entails and why it occurs. Only "once a company understands the risks of an undertaking, the owners or management can develop a strategy for containing them" (Bodine, Pugliese and Walker 2001).

4 Repudiation and the reasons for it

According to standard dictionary definitions, the term "repudiate" means to "refuse to accept or be associated with" and to "deny the truth or validity" of a particular aspect (*South African Concise Oxford Dictionary* 2002:992).

In terms of the *Laws of South Africa* (Volume 5(1), paragraph 237), repudiation "consists in words or positive conduct indicating an unequivocal intention on the part of either of the parties not to be bound, or not to be fully bound" by a contract. Examples of repudiation from the *Laws of South Africa* (Volume 5(1),

paragraph 239) include denial of the existence of a contract, contesting the terms of a contract, as well as a refusal to accept performance or to pay for it.

Non-repudiation services therefore aim to resolve disputes about the occurrence or non-occurrence of a claimed event or action, thereby ensuring that an individual cannot reasonably claim not to have taken an action. This means that an action is irrefutable. (Zhou and Gollmann 1997)

The general rule of evidence determines that, if a person denies a particular signature (which proves acknowledgement and acceptance of the transaction and thus prevents repudiation), the onus falls upon the relying party to prove that the signature is truly that of the person denying it (S v Boesak, 2000(1) South African Criminal Law Reports 633 (Supreme Court Appeal) paragraph 42; McCullagh and Caelli 2000). The term "deny" is synonymous with the term "repudiate". This position is supported by the definitions from the *South African Concise Oxford Dictionary* and the *Laws of South Africa* cited above.

In the context of a sales transaction, and taking the standard definitions of repudiation into account, the repudiation of a sales transaction entails that a customer (upon delivery of the goods) denies, refuses or renounces the order and his/her commitment or obligation towards the supplier.

If repudiation is to be addressed successfully, the first logical step is to consider the possible reasons why a customer would repudiate an order. The customer may do so because of the following:

- *An invalid and unauthorised order is fulfilled.* An unauthorised order that was placed (unbeknown to the customer, while using his/her details) is delivered to and rejected by the customer. This occurs because an order that a customer had not placed and/or approved was accepted and processed by the supplier.
- *The integrity of the order transaction is compromised.* Discrepancies arise between what the customer originally ordered and what is 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 originally approved and accepted by the two parties involved.

Now that repudiation and the reasons why it occur have been established, the next section explains the internal control measures typically present within a manual ordering system to address the subsequent repudiation of orders by customers.

5 Internal control measures to address the repudiation of orders in a manual system

In traditional manual business processes, where face-to-face transactions take place, authorisation and approval, which are 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 – the integrity of the transaction has not been compromised (Romney and Steinbart 2003:61).

In a manual system, the customer's signing of an order as proof of acknowledgement of placing the order and accepting the responsibilities arising from it ensures that a valid, signed "contract" exists between the customer and the supplier for the items specified in the order. Responsibility for and authorisation of the order are thus determined and defined. Before goods are sent to a customer, it is first established that an approved order exists (authorisation and validity are confirmed) and that the content of the goods to be delivered agrees with what was originally ordered (integrity of the transaction).

Upon delivery, the customer is required to sign a copy of the delivery note, by which the customer acknowledges that the goods, as specified on the delivery note, were taken into possession. Invoicing 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 these internal control measures are implemented, the risk that the customer will be able to repudiate the transaction successfully, in other words, deny either placing the order or receiving the goods, is reduced. Thus, there is no uncertainty regarding allocating responsibility for the payment of the monetary value of the items that were ordered and delivered to the customer concerned. The risk that the supplier will suffer losses as a result of repudiation is minimised.

However, the commencement of the digital era changed the situation substantially. In cyberspace the "intangibility and meta-physicality of its nature give rise to evidential issues" (Woo 2001). The King Report on Corporate Governance states that IT brought with it "increased risks and challenges that need to be addressed" by management, and that e-business initiatives have "implications for internal control systems" (King Report on Corporate Governance for South Africa 2002: Section 5, Chapter 4).

6 The digital environment and B2B open account systems

The Internet has changed the way in which two parties transact. Firstly, the parties involved in an Internet transaction might know little or nothing about each other's true identity, address, creditworthiness, reliability, etc. In such an environment, it is necessary for an effective business strategy, which also addresses IT, to be developed and implemented (Moscove 2001; King Report on Corporate Governance for South Africa 2002). E-business risk management, where e-business risk is identified and appropriately addressed (by implementing the necessary internal control measures), is essential.

Since taking the business world by storm in 1999 (Ward 2003), the popularity of business partners conducting business via the Internet (business-to-business, or so called B2B transactions) has been growing at a steady pace (Sairamesh, Mohan, Kumar, Hasson and Bender 2002). Research in a study named "Real Numbers E-Commerce Study Series", the results of which were published by ActivMedia Research in 2000, found that 50% of all businesses purchased online in 2000 (Bartlett 2000).

The eMarketer estimated in 2003 that $800 billion worth of purchases were made via B2B e-commerce in 2002 (Laudon and Traver 2004:81). It has been projected that all forms of B2B commerce will grow from 4% to 36% of total interfirm trading in the USA in the period from 2001 to 2005, or from $466 billion to $4,11 trillion (Laudon and Traver 2004:706).

In a study performed by The Business Software Alliance (BSA), chief executive officers of several of the world's top technology companies have indicated that a big future awaits B2B e-commerce (Bartlett 2001). It is predicted that by 2006 B2B purchasing will have grown to $5,4 trillion, or about one-third of the total interfirm purchasing at that time (Laudon and Traver 2004:81) and that by 2010, B2B e-commerce would be the most significant form of business transacting in terms of monetary value (Bartlett 2001).

As B2B transactions can easily amount to very substantial amounts, sound security and governance are essential. "Failure . . . can prove massively expensive. Financial repercussions can be astronomical, legal entanglements limitless, and the effect on business partners incalculable" (Garcia-Tobar 2001).

While e-commerce and B2B transactions were traditionally settled by means of credit card payments, other methods of payment have evolved. Open B2B accounts emerged, where payment for the B2B transaction does not take place immediately. In these systems a purchase is placed on account, to be settled by the customer (the other business) at a future time, as agreed upon by the two parties – usually at the end of the month, by means of an electronic funds transfer (EFT) – for example, Amazon.com which launched its "Amazon Credit Accounts" in 2001 (Morphy 2001; Enos 2001; Amazon.com).

The fact that immediate payment for the goods is not ensured creates a great risk that the supplier may suffer monetary losses as a result of the repudiation of the order by the customer. The existence of a relationship of trust between the two business partners is essential. It is even more important to ensure the validity of the digital B2B open account system order before it is accepted and executed. This would reduce the possibility of the order subsequently being repudiated by the customer, resulting in the supplier suffering losses.

7 Ensuring non-repudiation in a digital environment

Non-repudiation within a digital environment requires that neither the sender nor the receiver of a message must be able to deny the transmission of a message. 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).

The term "non-repudiation" crypto-technically means a service that provides proof of the integrity and origin of data in such a way that it could not be forged or subsequently refuted (McCullagh and Caelli 2000).

According to ISO/IEC 13888-1, -2 and -3 of the ISO, the purpose of non-repudiation in a digital environment is to deliver a service with an aim "to provide verifiable proof or evidence" of:

- Approval, Sending and Origin: proof of who is responsible for the approval of the content of a message, as well as proof of the sender of a message.
- 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, Knowledge and Delivery: proof that the recipient has received and recognised the content of a received message (McCullagh and Caelli 2000; Zhou and Gollmann 1997).

The two important reasons why customers would repudiate orders within a computerised environment are:

- *Invalid or unauthorised orders*, which were placed by gaining unauthorised access to the computer system, being accepted and processed by the supplier.
- After the initial acceptance of the order, unauthorised changes being made to the order, as a result of unauthorised access that had been gained to the order before/while it was being sent over internet communication channels – the *transaction integrity is compromised*.

If non-repudiation is to be achieved, the system of internal control should be designed and implemented to address these two aspects.

The internal control measures that are necessary to address the repudiation risk within a computerised environment depend greatly on the level of computerisation of the supplier's system. In systems in which the computer is only used on a small scale, some form of manual and/or user controls might be sufficient, whilst appropriate computerised internal control 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 acknowledging and pinning down responsibility. This means that the customer's signature may still remain the main source of authorisation – ensuring the validity of an order. Alternatively, electronic verification of available credit can be used.

To enable a legally binding and enforceable "contract" (order transaction) to be concluded between the buyer and the seller in a digital environment, traditional

business to consumer (B2C) and B2B systems require the prospective buyer (customer) to provide credit card information (which is immediately electronically verified with the bank), before an order transaction entered into via the Internet is accepted by the seller (supplier). This serves as the primary internal control measure to ensure that no orders are accepted and processed by the supplier before payment for the items can be confirmed. As illustrated earlier, this is not the case in B2B open account systems, substantially increasing the risk of repudiation and the possible negative effects thereof.

In a computerised system, the goods that are ready for dispatch are still physically compared to or electronically matched to the details of the order (which might only exist in an electronic format) before delivery takes place. In this process, authorisation for the goods to leave the premises and for the delivery to take place is established and possible unauthorised changes made to orders (compromising integrity) should be detected. Customers are still required to sign as proof of receipt on delivery of the items.

Invoicing takes place on the basis of the matched details of the signed underlying documents (order and delivery note), which links the responsibility for the transaction to a specific customer (by way of a signature), thereby reducing the probability that the customer will repudiate the transaction and deny responsibility.

In B2B environments in which orders are placed on open accounts, the controls referred to in the preceding sections would clearly not be appropriate to address the risk of repudiation.

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

According to ISO 13888-1, evidence relating to non-repudiation is information that "either by itself or when used in conjunction with other information is used to establish proof about an event or action" (Zhou and Gollmann 1997). The next section examines the evidence that would "prove" that a transaction (order) that is repudiated is, in fact, legally binding and thus irrefutable.

8 How to make digital B2B sales orders legally binding

Section 15 of The Electronic Communications and Transactions Act determines that, when the evidential weight of data messages is assessed, the following three matters must be considered (South Africa 2002):

- The manner in which the originator of the message was identified.

- ☐ The reliability of the manner in which the message was generated, stored and communicated.
- ☐ The reliability of the manner in which the integrity of the message was maintained.

This is supported by the following aspects that the court examines when considering the validity of a contract in digital form (Garcia-Tobar 2001):

- ☐ **Authentication**
  Proof must be supplied that the content of the digital contract is complete and unaltered. The order must truly be verified as the original that the two parties agreed to. There has to be proof that the digital communication involved in the business transaction actually comes from the parties from which it purports to come.
- ☐ **Signature**
  This is proof that the parties involved actually intended to sign the contract (agree to the order) and that parties that have the necessary authority within the respective organisations to do so entered into this agreement. The system for the exchange and signing of the digital contract has to 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 must sign identical versions of the contract. The contract should exist in a standard digital form. Each of the parties, when signing the contract, must submit the signature/(s) to the other party and be sure of delivery of the message. Proof should exist 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, should be kept confidential. Disclosure of the details of the transaction to unauthorised persons should be prevented.
- ☐ **Operational details**
  The contract must have been properly time-stamped and it must be verifiable that the individuals who digitally signed the contract had the authority to sign it at the time they did.
- ☐ **Record**
  Both parties must keep a copy of the contract in a tamper-proof and secure place or manner. Sufficient measures must have been 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 must be recorded at a digital notary service, without indicating where the supplier is located.

It can therefore be deduced that, to make a digital contract (of which a B2B sales order is one) legally binding and thus enforceable by the parties involved, the following two aspects relating to the order transaction are required:

- The authorisation and validity of the order transaction and the source from which it came have to be confirmed. The parties involved have to identify and authenticate each other when entering into the transaction to ensure that the transaction is valid and enforceable. This should be done before the B2B supplier accepts and processes the order, and is achieved by addressing the following two important principles (Information Technology and Control Guidelines 1998:219):
  - user identification – the means by which IT users identify themselves when interacting with technology; most often, this is a unique identifier, such as a logon or login ID. and
  - user authentication – the means by which a user is confirmed as being the valid owner of the user identifier that the user presents to the system.
- It has to be ensured that the content (integrity) of a message stays unchanged while it is stored and/or during communication. The order transaction information stored and/or sent over the communication channels should be protected from unauthorised access and/or changes to the order subsequent to the initial authorisation and acceptance of the order.

9 Objectives and recommended internal control measures to ensure non-repudiation

On the basis of the information contained in this article, the control objectives and/or principles defined in the *Control Objectives for Information and Related Technology* (COBIT®), and the *Trust Services Principles and Criteria* of AICPA/CICA, the most important objectives to ensure the non-repudiation of a specific B2B order transaction within an open account system are:

- The **identification** of the prospective customer/user.
- The **authentication** of the user before entering into an order transaction.
- Proper access control (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).
- Adequate **monitoring** (all attempts to gain unauthorised access or to make unauthorised changes are identified, logged and followed up).
- The **integrity** of the order transaction stored/transmitted over the communication channel must be guaranteed (ensure that no unauthorised changes are made to previously authorised transactions).

Now that the objectives to be achieved in order to prevent the repudiation of an order in a B2B open account system have been formulated, the internal control

measures that can assist businesses in achieving these objectives will be considered.

In addition to the internal control measures recommended by COBIT® and TrustServices, there are additional operational procedures and technology choices (Garcia-Tobar 2001) that can contribute to ensuring the non-repudiation of orders for B2B open account system suppliers.

Based on a literature review of the appropriate sources, the main categories of the relevant internal control measures that are necessary in a B2B environment to achieve the objectives set out above were identified. These internal control measures were linked to the objectives they would assist in achieving and are included in the matrix contained in Table 1.

The matrix in Table 1 was constructed as follows:

- ☐ The control objectives that would ensure the non-repudiation of orders in a B2B open account system are shown in bold and form the columns of the OBJECTIVES in the matrix.
- ☐ The appropriate internal control measures that would address the objectives formulated above and thus ensure non-repudiation appear as the rows of the matrix under the heading INTERNAL CONTROL MEASURES.

Table 1 Objectives and internal control measures to prevent the repudiation of B2B orders in open account systems

	Objectives				
Internal control measures	**Identification**	**Authentication**	**Limiting access**	**Monitoring**	**Integrity**
☐ Competent, reliable employees are in control of system security, or this service is outsourced to a reliable supplier of Security Services.			X		X
☐ User profiles are defined.	X				
☐ Users log on using unique user IDs and passwords.	X				
☐ Adequate control is kept 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		
☐ Users are logged out on request, or after 10 minutes of non-activity on the system.	X	X	X		

continued

Internal control measures	Objectives				
	Identification	Authentication	Limiting access	Monitoring	Integrity
☐ Control is maintained over the creation and amendment of passwords and user profiles	X				
☐ Log-on sessions are terminated after three unsuccessful attempts to gain access.	X	X	X		
☐ Unsuccessful attempts to gain access are recorded and followed up.					X
☐ Cryptographic techniques are used to sign and verify transactions.	X	X			
☐ All parties involved identify and authenticate one another before access is granted – for example, by making use of digital signature technology with public key infrastructure (PKI).	X	X			
☐ Trusted third party certificate authorities, for example, Verisign, Entrust and Digital Signature Trust, are used.		X			
☐ Input transactions with date and time stamping which can be verified by the source (user, terminal, IP address) are provided.		X			X
☐ Digital acknowledgement of receipt, with the specific date and time of transaction, is provided.	X	X			X
☐ Computer activity and messages (including user IDs and passwords) transmitted between users, between users and systems, as well as between systems, are protected by, 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;					X

continued

	Objectives				
Internal control measures	**Identification**	**Authentication**	**Limiting access**	**Monitoring**	**Integrity**
– privately leased lines, or virtual private networks with authorised users; and – bonded couriers and tamper-resistant packaging.					
☐ Virtual private network (VPN) software is used to authenticate outside users and control their access to the system.		X	X		X
☐ Firewalls are configured to control all access to the system.			X		
Firewall activities are recorded and reviewed daily.				X	
☐ All possible security breaches are followed up.				X	
☐ Intrusion-detection systems are used to monitor the system continuously.				X	
☐ All possible security breaches are followed up.				X	
☐ Independent third parties perform periodic reviews of system security and control. Results and recommendations are reported directly to management.	X	X	X	X	X
☐ E-business security software is subjected to periodic security audits that evaluate management, operating as well as technical controls.	X	X	X	X	X

10 Conclusion

Repudiation of orders by customers is a major risk faced by B2B suppliers who receive and fill orders in open account systems, as suppliers who have manufactured, packed, transported and delivered goods suffer monetary losses when customers repudiate these orders on delivery. When placing orders on open accounts, B2B customers do not have to provide credit card details that are immediately electronically verified before the transaction is accepted and executed by the supplier. (A quantification of the losses suffered by B2B suppliers as a result of orders placed on open accounts but which customers subsequently repudiate was beyond the scope of this article, but it could be an area for future research.)

The King Report on Corporate Governance (Section 1, paragraph 3) states that the management of the B2B supplier are primarily responsible for implementing the necessary internal control measures to address this particular risk. For management to be able to address the problem, it first has to understand the problem of repudiation and the reasons why it occurs. This article has explained the everyday problem of business risks that arise when transactions take place between business partners, and it defined and explained the particular risk of repudiation.

The reasons for the repudiation of orders were investigated and were found to be the result of one of two possible situations, namely:

- Invalid and unauthorised orders that are accepted and filled by a supplier.
- Subsequent unauthorised changes that are made to previously authorised order transactions.

The research has identified and formulated the most important objectives in preventing the repudiation of a specific B2B order transaction within an open account system. They are:

- The identification of the prospective customer/user.
- The authentication of the user before entering into a transaction.
- Proper access control, whilst enforcing adequate segregation of duties.
- Adequate monitoring.
- Ensuring the integrity of a transaction transmitted over the Internet.

These objectives, as well as the internal control measures necessary to ensure the non-repudiation of orders executed within B2B open accounts systems, are summarised in Table 1.

By implementing the internal control measures recommended in Table 1, the management of B2B suppliers would be able to reduce the risk of repudiation of orders placed on open accounts by customers to an acceptable level, thereby minimising the losses suffered by B2B suppliers as a result of repudiation.

Bibliography

Amazon.com. 2003. *Amazon Credit Account*, Accessed 21 July 2003, Available: http://www.amazon.com [21 July 2003].

Bartlett, M. 2000. *B2B Purchasing will double by 2002 – Study*, 28 November 2000, Accessed 29 July 2004, Available: http://www.newsbytes.com

Bartlett, M. 2001. *CEOs foresee glowing future for Internet e-commerce*, [Electronic], University of Stellenbosch Computer Database, Accessed 13 June 2003].

Bodine, S.W., Pugliese, A. and Walker, P.L. 2001. *A roadmap for risk management*, Journal of Accountancy, December 2001, p.65.

Boynton, W.C., Johnson, R.N. and Kell, W.G. 2001. *Modern Auditing*, John Wiley & Sons, 7th edition, New York.

Canadian Institute of Chartered Accountants (CICA). 1998. Accessed 2 June 2003, Available: http://www.cica.ca

Committee of Sponsoring Organisations of the Treadway Commission (COSO). 1992. Accessed 2 June 2003, Available: http://www.coso.org

Control Objectives for Information and Related Technology (COBIT®). 2000. 3rd edition. Information Systems Audit and Control Association (ISACA).

Enos, L. 2001. *Amazon extends credit to corporate buyers*, E-Commerce Times, 22 August 2001, Accessed 21 July 2003 Available: http://www.ecommercetimes.com

Garcia-Tobar, A. 2001. *Legalising B2B e-commerce*, Telecommunications Americas, [Electronic], March 2001, University of Stellenbosch Computer Database, Accessed 17 June 2003, Vol. 35, No. 3, p.116

Hartman, B. 2003. *Mastering web Services Security*, John Wiley and Sons, Accessed 22 June 2004, Available: http://legacy.netlibrary.com

Hunton, J.E., Bryant, S.M. and Bagranoff, N.A. 2004. *Core concepts of information technology auditing*, John Wiley & Sons, 1st edition, New York.

Information Systems Audit and Control Association (ISACA). 2003. Accessed 2 June 2003, Available: http://www.iasca.org

Information Technology Control Guidelines. 1998. 3rd edition. The Canadian Institute of Chartered Accountants (CICA).

King Report on Corporate Governance for South Africa. 2002. Institute of Directors (IOD). March 2002.

Laudon, K.C. and Traver, C.G. 2004. *E-commerce: business, technology and society*, Pearson Education, 2nd edition, Boston.

Laws of South Africa. Volume 5(1). First Reissue Volume. Butterworths, [Electronic], University of Stellenbosch – Library Resources, Accessed 22 June 2004, Available: http://www.lib.sun.ac.za/nxt/gateway.dll?f=templates$fn=default.htm$vid=MyLNB:10.1048/Enu

McCullagh, A. and Caelli, W. 2000. *Non-repudiation in the digital environment*, First Monday, 5(8), Accessed 21 July 2003, Available: http://firstmonday.org/issues

Morphy, E. 2001. *Amazon woos customers with new credit option*, ECT News Network, 5 November 2001, Accessed 21 July 2003, Available: http://www.ecommercetimes.com

Moscove, S.A. 2001. *E-business security and controls*, CPA Journal, [Electronic], November 2001, University of Stellenbosch Business Source Premier Database, Accessed 21 July 2003, Vol 71, No. 11.

Romney, M.B. and Steinbart, P.J. 2003. *Accounting Information Systems*, Prentice Hall, 9th edition, Upper Saddle River, New Jersey.

S v Boesak, 2000(1) South African Criminal Law Reports 633 (Supreme Court Appeal) paragraph [42].

Sairamesh, J., Mohan, R., Kumar, M., Hasson, L. and Bender, C. 2002. *A platform for business-to-business sell-side, private exchanges and marketplaces*, IBM Systems Journal, [Electronic], July 2002, University of Stellenbosch Computer Database, Accessed 13 June 2003, Vol. 41, No. 2.

South Africa. 2002. *Electronic Communications and Transactions Act of South Africa*, No. 25 of 2002. Pretoria: Government Printer, [Laws.]

South African Concise Oxford Dictionary. 2002. Oxford University Press, Cape Town.

Stallings, W. 1995. *Network and internetwork security – principles and practice*, Prentice Hall, Englewood Cliffs, New Jersey.

Tak, S., Lee, Y. and Park, E.K. 2003. *A software framework for non-repudiation services in electronic commerce based on the Internet*, Microprocessors and Microsystems, Vol. 27, pp.265-276.

Trust Services Principles and Criteria. 2003. Accessed 13 June 2003, Available: http://www.aicpa.org/assurance/trustservices

Ward, L. 2003. *The new face of B2B e-commerce*, E-Commerce Times, 22 May 2003, Accessed 21 July 2003, Available: http://www.ecommercetimes.com

Weber, R. 1999. *Information systems control and audit*, Prentice Hall, Upper Saddle River, New Jersey.

Woo, S.C. 2001. *Understanding electronic authentication*, [Electronic], July 2001, University of Stellenbosch EBSCO HOST Research Database Accessed 22 June 2004.

Zhou, J. and Gollmann, D. 1997. *Evidence and non-repudiation*, Journal of Network and Computer Applications, Vol. 20, pp.267-281.