

CHAPTER 1

INDEX

1.1	INTRODUCTION.....	2
1.2	BACKGROUND TO THE STUDY	3
1.2.1	FUNCTIONS OF THE DIFFERENT AUDITORS	3
1.2.1.1	The External auditor	3
1.2.1.2	The Internal Auditor	4
1.2.1.3	The Information Systems (IS) Auditor.....	4
1.2.2	BACKGROUND.....	5
1.2.2.1	A New-World Economy.....	5
1.2.2.2	Conclusion.....	7
1.2.3	THE GROWTH OF THE INTERNET AND INTERNET TRADING.....	7
1.2.3.1	Internet Growth.....	7
1.2.3.2	The Concerns and Opportunities for Businesses.....	9
1.2.3.3	Conclusion.....	11
1.2.4	ELECTRONIC COMMERCE (EC).....	11
1.2.4.1	What is Electronic Commerce?	11
1.2.4.2	EC Concerns and Payment Methods.....	13
1.2.4.3	Internet payment security	14
1.2.4.4	EC Importance Worldwide	15
1.2.4.5	Conclusion.....	16
1.2.5	ELECTRONIC COMMERCE AND THE IS AUDITOR	17
1.3	PROBLEM STATEMENT	19
1.3.1	RESEARCH OBJECTIVES	19
1.4	LITERATURE REVIEW.....	20
1.4.1	STANDARDS AND GUIDELINES	20
1.4.1.1	Conclusion.....	23
1.4.2	WEB ASSURANCE SERVICES	23
1.5	RESEARCH DESIGN.....	25
1.6	NATURE AND FORM OF THE RESULTS: DELIVERABLES.....	25
1.7	FACILITIES AND SPECIAL RESOURCES	26

1.1 INTRODUCTION

Essentially there are three types of audit. These are defined as follows (Vallabhaneni, 1991).

External Auditing is the process of accumulating, evaluating, and reporting the evidence collected by a competent and independent person during a review of economic activities of an entity using professional standards. For example, external auditors in the United States follow Generally Accepted Accounting Principles (GAAP) and perform audits according to Generally Accepted Auditing Standards (GAAS) promulgated by the American Institute of Certified Public Accountants (AICPA).

Internal Auditing is an independent appraisal activity established within an organisation as a service to the organisation. It is a control, which functions by examining and evaluating the adequacy and effectiveness of other controls. Internal Auditors are required to follow the professional standards issued by the Institute of Internal Auditors (IIA).

Information Systems (IS) Auditing is the process of evaluating and reporting the adequacy of system controls, efficiency, economy, effectiveness, and security practices, to assure that computer-related assets and information resources are safeguarded, that data integrity is protected, and that the system complies with applicable policies, procedures, standards, rules, laws, and regulations. The information systems (IS) auditor, needs to look at both automated and manual parts of the system because of their interfacing nature. Whether working as an internal or as an external auditor, this type of auditor should abide by the General Standards and Code of Ethics established by the Information Systems Audit and Control Association (ISACA). These standards should be followed in addition to those established by the respective professional associations (e.g., AICPA for auditors in the United States, and the IIA for Internal Auditors).

It is important for information systems auditors to carry out and discharge their duties and responsibilities, and to work in a manner consistent with the

Certified Information Systems Auditor's (CISA) General Standards and Code of Ethics.

This study will focus on the functions of the information systems auditor.

Certain other terms also need to be defined for the purposes of this research. The American Institute of Certified Public Accountants (AICPA) (1997) states: "Electronic commerce involves individuals as well as organisations engaging in a variety of electronic business transactions, without paper documents, using computer and telecommunication networks." An Internet payment system is described as a system of payment using the Internet as a medium to handle the payment side of trading transactions. Such a system will provide the user with comfort when goods and services are being acquired electronically.

1.2 BACKGROUND TO THE STUDY

1.2.1 FUNCTIONS OF THE DIFFERENT AUDITORS

The following section briefly describes the functions of the internal, external, and IS auditor (Vallabhaneni, 1991):

1.2.1.1 The External auditor

The external auditor evaluates the reliability and validity of systems controls, whether manual or automatic. The principle objective in this evaluation is to minimise the amount of substantive auditing, or testing of transactions required to render an opinion on financial statements.

The external auditor is responsible for testing the reliability of client computer systems and should have a special combination of skills and experience. Such an auditor must be thoroughly familiar with the attest function. The attest function encompasses all activities and responsibilities associated with the rendering of an opinion on the fairness of financial statements. Besides the accounting and auditing skills involved in performing the attest function, these external auditors must also have substantial CIS experience and training.

Audit firms are also using the services of qualified computer audit specialists. They generally work closely with audit staff members, though they may not be involved directly in the non-computerised portions of the audit.

1.2.1.2 The Internal Auditor

The purpose of the internal audit function is to assure management authorised controls are being applied effectively. Internal audit is not a mandatory function within a company. Internal audit is an internal control function, including continual activities for the monitoring and testing of all Computer Information Systems (CIS) functions. Of particular concern is the processing of data of financial relevance. Although it would seem logical, involvement in CIS has not been automatic for most internal auditors.

Top management must be concerned with the reliability of computer generated information upon which critical organisational decisions are made. In organisations in which management genuinely is concerned about this reliability, internal auditors are growing in stature. As internal auditors extend their capabilities and activities, their efforts become increasingly crucial to the examinations performed by external auditors. Thus, management typically assigns review, consultation, and testing responsibilities to the internal auditor. These responsibilities typically are broader in scope than those of the external auditor.

1.2.1.3 The Information Systems (IS) Auditor

The evaluation of computer information systems by auditors has generated the term information systems (IS) auditing. IS auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organisational goals effectively, and consumes resources efficiently. Thus, IS auditing supports the attainment of traditional audit objectives: attest objectives (those of the external auditor) that have asset safeguarding and data integrity as their focus, and management objectives (those of the internal auditor) that encompasses not only attest objectives but also effectiveness and efficiency objectives. The IS audit process is conceived as a force that helps organisations to better attain these objectives. What can be deduced from this is that the IS auditors can either fulfil their role in a capacity as external or

internal auditor. The overall objective of the IS audit will therefore agree with the overall objective of the internal or external audit (e.g., the overall objective of the external audit is to render an opinion on financial statements and the IS auditor will help to achieve this objective by providing assurance to the rest of the audit team regarding the reliance that can be placed on the computer systems).

The IS auditor's evaluation of systems, practices, and operations may include one or both of the following:

- Assessment of internal controls within the CIS environment to assure the validity, reliability, and security of information.
- Assessment of the efficiency and effectiveness of the CIS environment in economic terms.

To develop an audit approach for the IS Auditor regarding internet payment systems and internet payment security, it is necessary to provide background information on the change of business that has been taking place over the past few years. This study will highlight important aspects of the growth of the Internet and the role of businesses in the developments in Internet trading. This will be done in sections 1.2.2 and 1.2.3 below. Other aspects that need to be explained are electronic commerce including some of its different forms, and background on Internet payment security. This will be done in section 1.2.4 below. Section 1.2.5 then highlights the problems and challenges facing the IS auditor due to these developments.

1.2.2 BACKGROUND

1.2.2.1 A New-World Economy

It has become increasingly apparent in recent years that the earlier manufacturing economy is being replaced by an information economy. This conclusion is made based on the following statistics.

- It is estimated that "only 30 percent of all jobs in the USA are still in manufacturing. The rest (70 percent) are in the information and service economies" (*Agrireview*, 1998).

- Analysts also estimate that “more than 90 percent of the 1999 American GDP will come from the information and service economies. This tendency is now the norm throughout the First World” (*Agrireview*, 1998).
- The information era represents a fundamental shift in the priorities and customs of businesses all over the world. If we look at developments in America and other countries, the following important statistics emphasise this economic shift.
 - The US Department of Commerce (1998) states that “the IT sector’s share of the investment activity and the Gross Domestic Product of the United States grew from 4.9 percent of the economy in 1985 to 6.1 percent by 1990. This happened as the PC began to penetrate homes and offices”.
 - From 1993, with the burst of commercial activity driven by the Internet, until 1998, the IT share of the American economy rose to an estimated 8.2 percent (US Department of Commerce, 1998). With such rapid expansion, IT’s share of the total nominal GDP growth has been running almost double its share of the economy, at close to 15 percent.
 - In most traditional newly industrialised countries or NICs (in Latin America, Africa and Asia), GartnerGroup (as stated by Phifer et al, 1998) projects the following:
 Internet growth will be linked closely with economic development - in some cases, the former will be one of the main enablers of the latter. In NICs with high IT growth (such as India and China), taken as a percentage of the population having access to IT, it will likely be equal or greater to that of industrialised countries. Hunger for information in high IT growth countries will far outweigh certain cultural and political barriers found in more-industrialised nations. Already in those countries public Internet sites, such as public libraries or post offices, have terminals for the public to “surf the Net” at a nominal cost. This will likely create an Internet culture, even among those normally without access to Internet technology.

The factors in the manufacturing economy that made a business competitive were inexpensive inputs: raw materials, property, and labour. In the information economy the factors that will make businesses competitive in the future are information, knowledge, skills, and innovation. This implies higher-skilled and more expensive labour. It is already noticeable that the most successful economies have the highest labour costs and no significant raw materials.

1.2.2.2 Conclusion

The change in the world economies that has been brought on by the Internet implies a change in the ways of doing business. This has an impact on the function of the auditor. Auditors need to understand and recognise this change, and ensure their knowledge, standards, procedures, and methods develop with this change so that they will be able to meet the expectations of users of audit services. The role of the auditor regarding information in this changed worldwide situation will be further explained in section 1.2.5.

1.2.3 THE GROWTH OF THE INTERNET AND INTERNET TRADING

1.2.3.1 Internet Growth

When examining some of the statistics related to the growth of the Internet, it is further clear that a change is evident. Some of the statistics include the following:

- Already in 1997 an estimated “80 million people will be connected to the Internet in 1999 through more than 50 000 networks in more than 160 countries” (Robert Stephens & Co, 1997). It is further predicted that “every month over 5 000 new businesses and over 5 million new users become connected. As recently as 1991 not a single company was using the Internet. If the present rate of increase in Internet users could have been maintained, the number of users in the year 2003 would be equal to 125 percent of the world’s entire population. There will be an estimated 1 billion Internet users by the year 2000 and 2 billion by the year 2002” (*Agrireview*, 1998). It is clear that the present expansion of the Internet cannot be maintained. What can however be deduced from this growth is that the Internet is regarded as the nerve system of the new, free world market.
- According to Forrester Research, “in 1997 about 55 million Americans - more than one-fifth of the population - lived in households wired for e-mail. They send plus minus 150 million messages a day, or nearly three per person in this year. This is a huge leap from 1992, when e-mail messages totalled just 10 million a day” (Wladawsky-Berger, 1997). A worldwide survey showed that 87 percent of all enterprises (small, medium and large), across all industries use e-mail. All this proves that the Internet has begun transforming the way we live and work. It also

proves that the Internet is connecting millions of people to each other and to endless streams of information.

- Forrester Research (as quoted by KPMG, 1998) is predicting that “on-line activities (in Europe) will generate US \$1.2 billion in revenues in 1998, then grow to US \$64.4 billion by 2001.” GartnerGroup (as quoted by KPMG, 1998) recently found that “all enterprises in all industries see some level of Electronic Marketplace participation as good. At least 74 percent see participation as either necessary or critical to the future of their organisations.”

Some statistics (Garceau et al, 1998:14) related to Internet trading (on the World Wide Web) are summarised as follows.

- A market place in which almost all of its 250 000 stores have been in operation for less than a year.
- A market place that is expected to grow at a rate of 200 % per annum.
- A market with a total sales volume that will total US \$55 billion by the year 2000.

These are some of the more reliable estimates of the growth of its commercial activities. Whether the offer is wine, books, computers, airline tickets, or any other products and services, they can all be purchased today on the Internet.

The changes that have taken place in the telecom and information sectors in the last several decades are good examples of the changes that are brought along by information technology. The global network of computers, telephones, and televisions has increased the telecom sector’s information-carrying capacity dramatically. Statistics reveal the following:

In 1960, a transatlantic telephone cable could carry only 138 conversations simultaneously. Today, a fiber-optic cable can carry 1.5 million conversations at one time. Twenty-five years ago there were only about 50,000 computers worldwide; today that number is estimated at 140 million. And no communications medium has ever grown as fast as the Internet (the amount of information on the Internet is doubling every year) (Irving, 1998).

Other changes that took place in the information sector are found with laptop computers where today’s laptop computers weigh as little as 0.83 kilograms and are

many times more powerful than the R60 million mainframe computers of the mid-1970s.

1.2.3.2 The Concerns and Opportunities for Businesses

In its current state, the Internet is fundamentally a repository of human interest. And where there is interest, the chance of making a lot of money is usually not far off. Arriving at this conclusion are some of the largest companies in the world, as well as smaller entrepreneurial start-ups. They are all in a race to develop tomorrow's accepted standard for monetary exchange (Tibaldeo & Buben, 1996). Some examples of the acceptance of this "new type" of business are:

- General Electric uses the Internet for procurement;
- Dell estimates that it saves several million dollars a year by having basic customer service and technical support functions available on the Internet;
- Cisco Systems has saved approximately 17.5 percent of total operating costs by putting key business applications on the Internet.

It appears as if the path to electronic currency is being paved quickly, and tantalising visions of substitutes for paper currency and the leather wallet abound (US Department of Commerce, 1998).

A conclusion, after a recently released survey by the AICPA, states the following: "The Internet is dramatically changing the face of business today and is increasingly becoming a way for businesses to interact with their customers" (AICPA1, 1998).

Now we are entering a new century, and the information age is about change and about achieving new possibilities. This change will affect businesses. They need to understand it and, more importantly, take advantage of it. To illustrate this the following example is quoted.

Companies are quickly moving to utilise the expanded opportunities created by the Internet. For instance, Cisco systems, Dell computers, and Boeing's spare parts business report almost immediate benefits after putting their ordering and customer service operations on the Internet. They are so convinced of its benefit to their own companies and their customers that they believe most of their

business will involve the Internet in the next three to five years (US Department of Commerce, 1998).”

Businesses began using the Internet for commercial transactions with their trading partners in about 1995. The US Department of Commerce (1998) states that “early users already report significant productivity improvements from using electronic networks to create, buy, distribute, sell, and service products and services. By 2002, the Internet may be used for more than \$300 billion worth of commerce between businesses”. The US Department of Commerce predicts that

“internally, enterprises will use the Intranet for procurement and maintenance, repair and the overhaul of goods. Externally, enterprises will use the Internet for procurement of most goods and services. Through 2008, enterprises will evolve into extended enterprises, with business processes encompassing their suppliers and customers. Many enterprises have begun to redefine their business process boundaries and as a result are creating extended enterprises that encompass their customers, suppliers, and in some cases, their customers’ customers. Through 2002, one of the major trends in attempting to accomplish this will be the development of a new generation of extranet applications. By year-end 1999, more than 40 percent of large enterprises will extend their Intranets to include selected outside organisations for E-commerce-related applications” (Phifer et al, 1998).

Analysts believe that Internet retailing (where sales are actually completed on the Internet) “will grow quickly, but they vary widely on just how quickly. On the conservative end, it is expected to reach \$7 billion by the year 2000” (US Department of Commerce, 1998). Duncan (1996) believes that

To make the most of the potential of the Internet, retailers will have to overcome a number of challenges. Among others they will need to increase consumer confidence in relying on computer images and information to determine the quality and fit of a product, and simplify the process of returning defective or unwanted merchandise. They will also need to address the question of credit card security and consumer privacy. While the term is not always clearly understood, electronic commerce is becoming the tool used widely in today’s

marketplace to help organisations achieve superiority and a strong competitive edge.

According to Irving (1998) the “Internet is causing a lot of businesses to rethink how they do business.” Business owners and executives should ask themselves: “If the Internet, in its current state, had been around when the enterprise was founded, would you be running your business the way you are doing so today?” If the answer is no, why not change now? Other questions that should be asked are: “Can you develop a niche market? How can you compete effectively with off-line companies as well as other on-line companies?”

1.2.3.3 Conclusion

The commercial opportunities on the Internet are receiving regular publicity. But most users still shy away from buying through the Internet and are reluctant to use it for commercial purposes. The shopping experience through the Net is quite different from a regular one. And of course, there are also additional concerns such as security issues.

There is no doubt that organisations today are seeking new ways of doing business in an effort to deliver customised products and services, reduce paperwork, and build more efficient supply chains while reducing manual errors and obtaining better quality and customer service. One common organisational solution that is at the forefront of many people’s minds is electronic commerce.

1.2.4 ELECTRONIC COMMERCE (EC)

1.2.4.1 What is Electronic Commerce?

Electronic Commerce is defined (ECAMPO as quoted by Scacchi, 1995) as: “the paperless exchange of business information using EDI, E-mail, electronic bulletin boards, electronic funds transfer (EFT), and similar technologies. Electronic Commerce must seek to automate the generation, processing, co-ordination, distribution, and reconciliation of business transactions”. GartnerGroup (as quoted by Le Tocq & Young, 1998) predicts that: “Electronic Commerce is a market place and a technology that is in its infancy and growing fast”.

“Given the explosive growth of the Internet, most EC (Electronic Commerce) providers are migrating ...to the Internet in order to capture larger market shares. The World Wide Web, or simply the Web, has become the vehicle of choice for conducting commerce over the Internet because of the user-friendly and rich multi-media interface provided by Web browsers” (Ghosh, 1997).

EC is not just for big corporations. In fact, it provides exciting possibilities for small companies and entrepreneurs to tap into markets around the world. Moreover, it enables the sharing of valuable information and resources. This is proven by the following example given by Irving (1998).

Women Inc. (a non-profit organisation devoted to helping women business owners succeed) and AT&T announced a partnership that will greatly help women entrepreneurs and could serve as a model for other groups. AT&T has provided Women Inc. with a \$25,000 grant to develop and host a Web site that will give Women Inc. members data space for business transactions, space to sell their products and services, the opportunity to “ask the expert” business-related questions, and the ability to register for conferences. Through the Web site, members also have access to a host of services.

The Internet and other communications networks are lowering entry barriers to commerce, enabling both small and large firms as well as consumers to engage in and benefit from electronic commerce. Electronic commerce is already generating important sales and savings for businesses. For example: “The on-line bookseller Amazon.com's increasing share of the bookstore market (by offering discounts up to 40 percent) forced major bookstore chains like Barnes & Noble and Borders Books to go on-line” (Irving, 1998). Other statistics from the US Department of Commerce (1998) shows that: “Federal Express delivery service saved as much as \$10,000 a day in 1996 by moving some of its customer service to its Web site; Dell Computer now sells \$1 million worth of PCs every day on the Web; General Electric buys \$1,000 million in materials from suppliers on-line and saves money by streamlining the process and opening it up to more competition.”

Electronic commerce is also changing the way in which banks and consumers interact and transact. Electronic commerce provides consumers with the ability to

bank, invest, purchase, distribute, communicate, explore, and research from virtually anywhere where an Internet connection is available.

1.2.4.2 EC Concerns and Payment Methods

The vast growth potential for electronic commerce in the banking and financial services industry is tempered by legitimate concerns over the security of such a system. Most diners in a restaurant are not too concerned about the possibility of a waiter keeping an imprint of their credit card number. Similarly, buyers usually feel comfortable about giving credit card numbers over the phone to an operator. The question arises as to why should e-commerce be any different? The answer lies in the scale of the fraud or theft possible by exploiting flaws in the software systems that facilitate e-commerce transactions. The very nature of computing includes the ability to amplify many-fold the effect of a simple software error into large-scale fraud, theft, or security intrusions. A simple error in configuring a commerce site's Web server has a possible effect of compromising thousands of credit card numbers, resulting in the quick and wide distribution of these numbers.

A recent criminal case (Ghosh, 1997) illustrates this vividly:

Carlos Felipe Salgado Jr. pleaded guilty to have been paid \$260,000 in an FBI sting for a diskette containing personal information for over 100,000 credit-card holders. Salgado allegedly obtained the data by hacking into company databases through the Internet. To protect e-commerce systems from these types of abuses, the systems must be secured systematically.

The benefits of providing goods and services over the Internet are immediately apparent. However, placing a server on the Internet also opens the potential for malicious criminals to break into systems, steal files, deny service and possibly destroy the host systems.

Electronic commercial transactions are concluded by use of credit cards, electronic cash, smart cards or stored value cards and digital money, amongst others. Digital money, in its various forms, is already being used in e-commerce on the Internet. Some of these e-commerce systems such as eCash and Smart cards are considered to be electronic money. Other systems employ traditional forms of

payment such as credit cards and cheques, but with enhanced security to ensure integrity, authenticity and non-repudiation of transactions.

Today the most common form of payment on the Internet is the credit card. The use and misuse of credit cards on the Internet for payment has received significant attention in the press. As an example, Garceau (Garceau et al, 1998) quotes the following case.

In March 1997, it was reported that approximately 100 000 credit card numbers were stolen from a company in San Diego. Someone broke into the system of an Internet service provider and installed a packet sniffer. This sniffer was configured to identify and record specified blocks of information such as credit card numbers.

In theory it is possible to steal information flowing from the Internet by using a sniffer. From the above examples it is clear that good security is required.

1.2.4.3 Internet payment security

According to Denny (1997) “one of the biggest challenges in the development of electronic commerce has been for banks and merchants to overcome the issues of customer identification and account verification for online purchases.” While the credit card systems have a process in place to verify and authorise transactions, the Internet poses challenges for merchants to not only validate that funds are available in an account, but to positively identify that the customer is in fact authorised to use that account for purchases.

In the physical world, merchants validate the identity of the account holder by comparing the signature on the credit card with the signature on the sales slip. But in a virtual world, where the customer is not present, the merchant does not know if that person is authorised to use the account number provided for the transaction. The danger in the electronic commerce environment is that, without additional controls, the exposure to losses from fraudulent usage is exponentially greater.

Visa and Mastercard, the two leading credit card companies, would like to guarantee that credit card information transmitted over the Internet is very secure. Towards this

purpose, Visa and Mastercard, in a joint business venture, have proposed the SET protocol. The RSA Corporation was chosen to develop the specifications for SET and implement the software needed to provide a secure environment for credit card usage on the Internet. The goal of the SET protocol is to “provide on-line transaction security at a comparable or better level than available in person-to-person, mail, and telephone based credit card transactions, by using cryptographic techniques. These state of the art techniques will provide confidentiality of financial data, ensure payment integrity, and authenticate merchants, banks, and cardholders” (Garceau et al, 1998). These techniques are all essential control requirements for EC security.

Another example of Internet related security development is Public Key Infrastructure (PKI). PKI is the combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transaction on the Internet.

PKI provides the following controls. Authentication of identity, verification of integrity, assurance of privacy, access authorisation, authorisation of transactions, and support for non-repudiation.

PKI lets an enterprise take advantage of the speed and immediacy of the Internet, while protecting business-critical information from interception, tampering, and unauthorised access.

1.2.4.4 EC Importance Worldwide

The following quotations from the report of the Institute of Chartered Accountants in Scotland (ICAS)(1998) recognise and re-emphasise the importance of electronic commerce, and the developments in the electronic commerce field.

- “In May 1998, the G8 Finance and Foreign Ministers met in Birmingham, UK to discuss the commercial effect of e-commerce throughout the world. At this meeting they undertook to ‘...work with the international institutions and the private sector to offer the best opportunities for the future: a predictable and stable environment and a seamless, decentralised global marketplace where competition and consumer choice drive economic activity...’ “

- “In October 1998, the Organisation for Economic Co-operation and Development (OECD) published a document entitled *Electronic Commerce: Taxation Framework Conditions*. The OECD set up five working groups to implement the Taxation Framework for e-commerce, which was agreed at a conference in Ottawa. This, in turn, drove home the message that large-scale electronic commerce was just around the corner and the world needed to make sure that it was ready for it. In The Tax Journal of 9 November 1998, C Anne Fairpo wrote ‘...Electronic commerce is growing; recent predictions estimate that over US\$300 billion of business will be carried out electronically in the year 2000...’”
- “Since then, various Governments, including the UK, have been working to meet the challenges posed by electronic commerce and to ease the path for businesses and consumers alike.”

1.2.4.5 Conclusion

The emergence of markets on the Internet has had a dramatic impact upon the traditional ways of doing business. The Internet provides a network that allows individuals and enterprises to connect in a way never before believed possible. It provides a framework that allows the convergence of voice, data, and broadcast, all of which have been (and mostly still are) discrete. It brings customers and merchants closer together. Yet, it also introduces new problems, such as the following.

- How is the customer to know to whom he is giving his credit card detail?
- What if the customer wishes to pay with cash?
- How does the merchant know that this is a legitimate customer order?
- What physical evidence does either customer or merchant have of an order being placed?

As mundane as these problems may appear, they represent a formidable challenge to the growth of e-commerce. If e-commerce is to succeed, it is necessary to find in the electronic world of the Internet, answers to these questions. Both customers and merchants must have the same level of confidence in purchase and sales transactions conducted over the Internet as they do when they buy or sell goods over the counter, by mail, or over the phone.

Here the auditor plays an important role by understanding the issues, analysing the effects of these issues on the risks and controls in an organisation, and recommending solutions. In order for an auditor to fully understand the risks, impact, and possible controls available in an Internet payment system it is necessary to understand the EC environment, including the development of Internet payment security systems.

1.2.5 ELECTRONIC COMMERCE AND THE IS AUDITOR

The functions of the different types of auditors have been highlighted in section 1.2.1 above. The role of the IS auditor in electronic commerce has been defined as follows.

Electronic commerce presents the IS auditor with challenges and opportunities. Its emergence will cause people to rethink the way organisations do business, and will force them to focus on enterprise-wide issues and technological solutions. A focus on business processes will be necessary to understand and evaluate an organisation's electronic commerce strategy (including electronic commerce objectives and investments), process re-engineering strategies, change management issues, and operational improvements that affect business transactions. A focus on technology considerations will be necessary for evaluating connectivity/hardware issues, information protection strategies, and application quality considerations (Tibaldeo & Buben, 1996).

Electronic commerce integrates many technologies, both in hardware and software. In addition, information protection mechanisms must be included in the design. Implementation and maintenance of the network architecture must provide more secure and manageable access to public services and reduce associated risks. The protection mechanisms, which are part of the total electronic commerce picture, may include firewalls, data encryption, digital signatures, and time stamping.

Tibaldeo (Tibaldeo & Buben, 1996) is of the opinion that "most IS professionals are familiar with several electronic based payment systems such as credit cards, direct deposits, and bank-to-bank transfers". The media and Hollywood films are probably responsible for escalating people's expectations regarding these payment systems.

These films produce a perception of electronic payment methods involving virtual reality and biometric authentication systems. Tibaldeo (1996) further believes that “although authenticating purchases at the virtual grocery store by way of retina scan may be far into the future, technology conscious merchants and consumers are carefully watching the development of several forms of electronic payment. Several emerging electronic payment models such as digital cash, electronic cheques, encrypted credit cards, and third-party processing transactions are poised to take the Internet by storm”. IS audit professionals need to understand how the strengths and drawbacks of these models compare.

There are other aspects relating to the controls in Internet related systems that could affect the auditor. The Internet today is a vast frontier of unknown elements including new types of software, new discoveries of security flaws, and unfriendly neighbours. The most secure technical solution to preventing attacks launched from the Internet is to unplug the network from the computer. This solution is not viable in today's business climate. Rather, the components that comprise e-commerce systems must be adequately secured.

Paliotta (1995) is of the opinion that “auditors need to take an objective look at the new technological advances, evaluate the risks associated with them, and work with management to establish controls that reasonably assure the new technological world order will be a safe place to “live” in.” The risks can be, and must be controlled.

Today's IS auditors are living in exciting and interesting technological times. Technological advances provide major competitive advantages to those with the ability to harness, utilise and control them – or they are a curse to those who cannot. With opportunity comes threat, and the audit, control, and security professionals will have an important role in helping management safely navigate through the new world order and to use it to its best advantage.

The question now arises: What is being done by auditors all over the world to address the risks of Internet related systems, and to provide assurance to customers and management in this regard? One development in this area is the Web Assurance Services provided by certain audit institutions. Web Assurance Services are discussed in more detail in the Literature Review section (1.4.2) of this document.

1.3 PROBLEM STATEMENT

1.3.1 RESEARCH OBJECTIVES

Organisations are facing mounting pressure from increased competition, especially in developments in Internet trading. As shown in the previous sections, certain companies have been forced to adopt an approach towards Internet trading in order to survive: e.g. the example of Amazon.com mentioned in section 1.2.4.1. The change in the business approach or processes introduces new risks to organisations. Management of an organisation has to be aware of the new risks introduced through Internet trading and therefore look towards the IS auditor to inform them regarding the risks and controls.

In the rapidly changing world of Information Technology and specifically the Internet, the IS auditor needs to keep up to date with developments and to keep management informed of new risks facing an organisation. The IS auditor also needs to keep up to date with the ever-increasing developments in the wider information technology field, and when it involves the possible expansion of audit services, such as certifying the integrity of a web site, then the auditors must become familiar with the relevant concepts.

The nature of technology used in electronic commerce as well as the regular flow of new developments in this technology area, result in limited articles being available to assist in understanding this environment. Although articles have been written on various of the technical aspects of electronic commerce or on parts of electronic commerce, the auditor needs to bring the technical aspects into line with the auditor's function and role in an organisation. This research therefore aims to cover the technical aspects as well so that a complete understanding is possible.

This study aims to develop a guideline or approach for IS auditors when they are confronted with the audit of an *electronic commerce environment*, especially an audit in Internet payment security.

1.4 LITERATURE REVIEW

1.4.1 STANDARDS AND GUIDELINES

The following Auditing Standards and Guidelines prescribes the role of the auditor when confronted with a Computer environment (Vallabhaneni, 1991):

- ISACA defines IS Auditing as follows: “the process of evaluating and reporting the adequacy of system controls, efficiency, economy, effectiveness and security practices to assure that computer related assets and information resources are safe-guarded, that data integrity is protected, and that the system complies with applicable policies, procedures, standards, rules, laws, and regulations.”
- *ISACA General standard No 4* regarding skills and knowledge reads as follows: “The information systems auditor is to be technically competent, possessing the skills and knowledge necessary in the performance of the auditor’s work.”
- *ISACA Standard No 5* states: “The information systems auditor is to maintain technical competence through appropriate continuing education.”
- Guideline 3.407 – Auditing in a Computer environment, states: “When auditing in a computer environment, the auditor should obtain a basic understanding of the fundamentals of data processing and a level of technical computer knowledge and skills which, depending on the circumstances, may need to be extensive.”
- International Federation of Accountants (IFAC) statement No 15 relating to Auditing in an EDP environment states: “When auditing in an EDP environment the auditor should have an understanding of computer hardware, software and processing systems sufficient to plan the engagement and to understand how EDP affects the study and evaluation of internal control.”
- IFAC20 states: “The auditor should conduct a preliminary evaluation of those general EDP controls on which he believes it might be effective and efficient to rely in conducting the audit.”

The above standards highlight the duty of the auditor, which is to understand the concepts and fundamentals of an electronic commerce environment when confronted by the audit of such an environment.

Whilst no universal definition of EC exists, it is clear that it is all about the method of communicating over networks between buyers and sellers of goods or services. In

order to achieve this, new technologies are constantly evolving. It is important that they are understood together with the related management issues of security and control. The Institute of Chartered Accountants of Scotland (ICAS, 1998) states that

“The extent of electronic trading is presenting businesses with unique challenges and presents the audit profession with a number of similar challenges and opportunities. Successfully managing the transition to electronic commerce demands overcoming a number of significant issues, including not only making the technology work, but also re-engineering existing business models and business processes. The change can so fundamentally affect an organisation that the evolution involves all aspects of the business from procurement to marketing and from finance to the audit.”

As soon as an organisation considers EC and challenges their own business model, it provides auditors with an ideal opportunity to reassess the way the audit is carried out. To understand the risks, auditors need to ensure that the business processes being developed support the client's strategies, and that control procedures are integrated from the start. Because the business is susceptible to fundamental change, so are the risks involved. One such example is the transformation of business relationships.

The risks and concerns as identified by the ICAS (1998) are summarised as follows.

- In the rush to the Web, it is important that the business does not overlook the issue of financial control of the process. Financial control contains several key elements including the security of systems underlying the process and the accuracy of information.
- The most notable issue concerning consumers and businesses alike regarding e-commerce is security, especially that of the Internet. The Internet is known for its lack of security. Unless encrypted during transmission, messages can be intercepted and read by third parties. In the case of sensitive information, such as credit card numbers, unintentional disclosure to unauthorised parties could result in significant financial loss.
- New ways to conduct electronic business often means connecting to other public or private networks. Trusted business partners are not the only ones shown the way to client's electronic systems: electronic vandals, criminals and other threats

are also given access. The advent of the "Secure E-commerce" Bill in the UK brings further risk in that it suggests that the government retains the right to access encrypted information without the knowledge of the business, and prevents service providers from tipping them off.

- Evaluation of the security environment surrounding a client's systems becomes key to providing audit assurance that the data which forms the basis of the financial statements is complete and accurate. Auditors have traditionally reviewed data file access and program change controls. In an e-commerce environment, this has expanded to cover increasingly detailed controls such as application, access, authentication controls as well as physical and logical access.
- A significant impact of electronic trading on businesses is that there is less margin for error - transactions have to be right first time, every time - especially those where funds are being transferred. This combined with the implicit loss of paper trail, means that processes have to be well controlled and have a clear electronic audit trail. For example, current requirements to hold financial information for a period of time extend to electronic information. This has significant ramifications in an electronic environment and would require historical information to be recoverable even if systems have changed. Recoverability and contingency planning in the event of disaster are also significant concerns.

In future, an explosion of e-commerce will require all auditors to have a greater understanding of the types of risks this kind of trading brings.

Further evidence of the importance of electronic commerce as seen by the Accounting Associations is found in the following statements (Elliott & Pallais, 1997).

- With accounting and auditing income flat for the last seven years, the CPAs profession's greatest opportunity for growth lies in new assurance services. (This includes the electronic commerce area).
- A variety of research would also help the profession's expansion into new assurance services. One of the kinds of research mentioned is criteria for assessing the integrity and security of electronic commerce. The estimated market for electronic commerce assurance services alone is between \$ 1bn and \$11bn. Systems and information technology naturally plays a prominent role in the new assurance services. They are part of how information for decision

making is gathered and deployed and used in transactions. More opportunities will open up as the information technology revolution continues. Practitioners' information technology skills and knowledge will affect not only the range of new assurance services they can avail themselves of, but also the way they adapt their traditional services to changing circumstances.

- The 'new' role of the auditor is also defined as follows: "The traditional audit with its standard report and measurement criteria designed to enhance comparability across all reporting entities, is a general-purpose service. The specific information needs of individuals and groups will dictate new assurance services. To identify these needs, practitioners will require a new mind-set, communications skills, business knowledge and the capacity to make inferences from relationships between business circumstances and economic and industrial trends."

1.4.1.1 Conclusion

The use of electronic commerce in business involves many risks and concerns. This will require auditors to have a greater understanding of the risks and controls to mitigate the risks. The conclusions reached by the Accounting Associations above shows the need for an understanding of the electronic commerce area as well as the need for the auditing profession to become involved in providing electronic commerce related assurance services as part of their duties.

1.4.2 WEB ASSURANCE SERVICES

The American Institute of certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) joined forces to develop and offer a new business-to-business electronic commerce assurance service. Accounting firms that are duly licensed by the AICPA or CICA provide assurance services to clients and place the WebTrust seal of assurance on their clients' World Wide Web sites. Users who engage in electronic commerce with a company that displays the seal are provided with certain assurances regarding compliance with disclosed business practices, integrity of electronic commerce transactions, and protection of private information. "This bold initiative by the AICPA and CICA is a remarkable event in the history of the accounting profession, as it sets the stage for the continued entry of

many new and exciting assurance services well into the 21st century” (Hunton et al, 1998).

The WebTrust service was designed in the US and was launched in the US and in Canada in 1997. It has quickly been accepted by the business community as a leader in its field and although not unique, provides the greatest breadth of review available to date. It is soon to be available in Australia, New Zealand and mainland Europe. All countries adopt the same approach to provide an international solution to a global issue. Specially trained auditors examine Web-site operator’s business methods and practice as they have been applied over a period of time (usually three months) and assess the adequacy of security arrangements over the Web-site itself. The findings are compared with laid down principles and criteria and, if acceptable, a seal of approval is affixed to the Web-site. The “Principles and Criteria” cover the three major areas of concern to consumers in their dealings with a Web-site. According to ICAS (1998) these are:

1. Is the Web-site safe from viruses or other electronically-born dangers on interrogation?
2. Is private information passed to the Web-site kept private and confidential?
3. Do I get the goods I ordered delivered in good condition and if not can I get my money back?

The reviews are repeated at regular (typically three monthly), intervals to ensure the standards are maintained.

Information systems auditors play a key role in providing web assurance services, particularly in the area of information protection. Assurance services are performed under the guidance of AICPA Professional Standards AT100 in the USA and CICA Handbook Section 5025 in Canada. As such, accounting practitioners are charged with providing an examination level engagement before placing the seal on the client’s web site. An engagement performed at the review level is insufficient. This means that practitioners will have to evaluate and test rather sophisticated internal controls over information technology, including transmission protocols and computer security. Given the competitive advantage of information systems auditors in this regard, it is likely that general practitioners will recognise the value and seek the help of CISA certified professionals when conducting assurance examinations on web

sites. It is therefore vitally important that information systems auditors be adequately informed and trained in the area of WebTrust assurance in order to leverage their intellectual capital in this growing service area.

1.5 RESEARCH DESIGN

The focal points of this dissertation are twofold. Firstly there is a literature survey of existing authoritative (print based) articles (books and literature), studies and research done on the development of electronic commerce. Due to the dynamic nature of electronic commerce, this survey will also be done on information published on the Internet, especially on the Web-sites of recognised professional bodies and institutions. The literature survey will also focus on developments in the audit area regarding the Internet and it's environment.

Secondly, it will involve the development of an audit approach based on the information gathered in the literature survey.

1.6 NATURE AND FORM OF THE RESULTS: DELIVERABLES

The results will comprise firstly the identification of possible types of electronic commerce and their development. From this identification the role of auditors in the area of electronic commerce will be defined. Specific emphasis will be made on Internet payment systems and Internet payment security. This will include a theoretical explanation of these electronic commerce concepts which is available for educational background information for an IS Auditor. These facts will be obtained through the literature survey.

Secondly, the approach that an auditor should take when confronted with the evaluation of an Internet payment system or Internet payment security environment will be defined. This will include considerations for the IS auditor that are also applicable to companies that are considering EC as an option and that are concerned about Internet payment security. These considerations will be presented in a separate Appendix to this study, due to the high volume of considerations in such a complex environment.

1.7 FACILITIES AND SPECIAL RESOURCES

Due to the complex nature of electronic commerce and the fact that it is regarded as being at the forefront of technological development, the availability of information on this subject is restricted to the Internet and a limited number of articles and research papers done in this regard. The Internet is therefore one of the main sources of information.

EC and Internet security involves many technical terms used throughout this dissertation. A separate Appendix will be provided to explain the most important and most used terms used in this dissertation.