AN AUDIT APPROACH OF THE INFORMATION SYSTEMS AUDITOR IN AN ELECTRONIC COMMERCE ENVIRONMENT WITH EMPHASIS ON INTERNET PAYMENT SECURITY

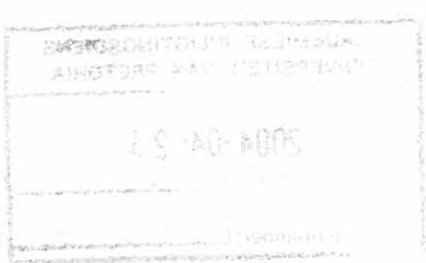
BY

PIETER STEFAN BEZUIDENHOUT

SUBMITTED IN PARTIAL FULFILMENT OF REQUIREMENTS FOR THE DEGREE MCOM (COMPUTER AUDITING)

IN THE FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES UNIVERSITY OF PRETORIA PRETORIA

OCTOBER 2002



Foreword

I have been in the IS auditing field for more than 10 years and have worked for a number of international companies as a consultant and an auditor. During the past few years I noticed the growth of Electronic Commerce and realised that it is an area of high risk to any organisation, and that due to the complexity of the technologies involved, requires a great amount of skill from IS auditors. Especially in the areas of EC payment security there seems to be a lack of readily available information to help the IS auditor obtain a comprehensive overview of the risks involved and the controls required. I hope this study will provide pertinent information to IS auditors, assisting them to understand the concepts around EC payments security. I trust that it will furthermore enable them to provide the professional service required by the people they report to, as well as fulfilling the professional standards required by the organisations to which they belong. With this better understanding IS auditors should be able to address the control concerns of organisational management, and conduct more efficient audits. The improved control environment which results from the work of the IS auditors should in turn ensure fewer mistakes and reduce the risk of fraud in organisations.

I would like to express my sincere gratitude to the following people. Any errors or omissions are mine and mine alone:

- My study leader, Prof Dr JD Gloeck, for the endless hours spent in reading through the content; for his encouragement and the valuable feedback provided, and for helping to overcome the concept of distance learning through numerous e-mails and phone calls;
- The Information Systems Audit and Control Association, which provides a wonderful source of information and a professional service to their members through their website;
- Mr. Chris Davies for his support in editing the document and for providing general advice;
- My wife, Rosemary for her support, encouragement, and assistance with sorting my sources and reading through all the chapters and making sure the concepts are understandable and clear to non-auditors as well;

- The millions of people who provide us with the wonder of technology and a wonderful tool such as the Internet.
- My Heavenly Father, the Source of everything that is life, for giving me the knowledge, strength and insight to complete this study.

NEW YORK
14 October 2002.

Contents

LIST OF APPENDICES

LIST OF TABLES USED

Summary

Candidate: Pieter Stefan Bezuidenhout
Study Leader: Prof. Dr. J.D. Gloeck
Department: Department of Auditing
Degree: Magister Commercii
Title: An audit approach of the information systems auditor in an electronic commerce environment with emphasis on internet payment security

Electronic Commerce (EC) is a growing business option and due to the "openness" of the underlying technologies used for EC, introduces new risks and new technologies that require sophisticated and sometimes very technical controls to be implemented. The role of the IS auditors is to ensure that they are technically competent to understand the impact of new technologies on the control environment and at the same time IS auditors need to be able to communicate the audit results to non-technical management.

In this study the following framework, supported by detailed information and procedures for each step, is provided to assist the IS auditor to formulate an appropriate audit approach for an EC payment security audit:

- Gathering of background information related to EC payment security.
- Highlighting the risks in this environment.
- Identifying possible controls that will minimise the risks.
- Attending to various audit considerations that should be addressed by the IS auditor (these considerations are based on the underlying technologies, general controls, and EC-specific issues e.g., PKI, digital certificates, etc.).

The study highlighted the fact that the IS auditors should understand that they can not be experts in all the different technologies related to EC payment security. They should, however, equip themselves with the knowledge to understand the risks involved with new technologies and they should have a sufficiently in depth background exposure to technology to understand the controls required to address the risks. Results of previous audit procedures also play a significant role in shaping the IS auditor's approach when auditing in an EC payment security environment.

This thesis provides IS auditors with a framework for conducting an EC payment security audit. After considering and implementing the elements of the framework developed in this study in an EC payment security audit, the IS auditor has to perform the actual audit tests, evaluate the results, and report the findings. Detailed audit considerations have also been provided to assist the IS auditor in collecting information and in developing an audit program.

Opsomming

Kandidaat: Pieter Stefan Bezuidenhout
Studieleier: Prof. Dr. J.D. Gloeck
Departement: Ouditkunde
Graad: Magister Commercii (Rekenaarouditering)
Titel: 'n Ouditbenadering van die inligtingstelselouditeur in 'n elektroniese handel omgewing met klem op internetbetalingsekuriteit

Elektroniese handel (EH) is 'n groeiende besigheidsopsie en as gevolg van die "oop" struktuur van die onderliggende tegnologieë wat gebruik word in EH, word nuwe risiko's en nuwe tegnologieë bekendgestel wat die implementering van gesofistikeerde en telkens baie tegniese kontroles vereis. Die rol van die inligtingstelsel (IS) ouditeure is om te verseker dat hulle tegnies bekwaam is om die impak van die nuwe tegnologieë op die kontrole omgewing te verstaan, en terselfdertyd moet IS ouditeure in staat wees om die resultate van die oudit aan nie-tegniese bestuur te kommunikeer.

In hierdie studie word die volgende raamwerk, wat ondersteun word deur gedetailleerde inligting en prosedures vir elke stap, verskaf om die ouditeur by te staan met die formulering van 'n toepaslike ouditbenadering vir 'n oudit van EH-betalingsekuriteit:

- Versameling van agtergrondinligting in verband met EH-betalingsekuriteit.
- Identifisering van die risiko's in die omgewing.
- Identifisering van moontlike kontroles wat die risiko's sal minimaliseer.
- Gee aandag aan die verskeie ouditaspekte wat deur die IS ouditeur oorweeg behoort te word (hierdie oorwegings is gebaseer op die onderliggende tegnologieë, algemene kontroles en spesifieke EH-kwessies byvoorbeeld, openbare sleutel infrastruktuur (PKI), digitale sertifikate, ens.).

Hierdie studie beklemtoon die feit dat IS ouditeure moet verstaan dat hulle nie deskundiges kan wees in al die verskillende tegnologieë wat met EH-betalingsekuriteit verband hou nie. IS ouditeure behoort egter hulleself toe te rus met die kennis om die risiko's wat by die nuwe tegnologieë betrokke is, te verstaan en

hulle behoort voldoende diepte agtergrondblootstelling aan die tegnologieë te hê om die vereiste kontroles wat die risiko's sal beperk, te verstaan. Die resultate van vorige ouditprosedures speel ook 'n belangrike rol in die formulering van die ouditeur se benadering wanneer 'n oudit uitgevoer word in 'n EH-betalingsekuriteitomgewing.

Hierdie studie verskaf 'n holistiese benadering aan die IS ouditeur vir 'n EH-betalingsekuriteitoudit. Nadat die elemente van die raamwerk wat in hierdie studie van 'n EH-betalingsekuriteitomgewing ontwikkel is, oorweeg en geïmplementeer is, moet die IS ouditeur die werklike oudittoetse uitvoer, die resultate evalueer en bevindinge rapporteer. Detail oorwegings is ook verskaf om die IS ouditeur te help tydens die proses van inligtingsversameling en die ontwikkeling van die ouditprogram.

CHAPTER 1

INDEX

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 deducted 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.

CHAPTER 2

THE ROLE OF THE AUDITOR DEFINED

INDEX

2.1 INTRODUCTION

The purpose of this study is to develop an audit approach that will assist the IS auditor when auditing Electronic Commerce (EC)/ Internet payment security. In order to achieve this purpose an understanding of the role of audit and more specifically the role of the IS auditor is required. As stated in the introductory chapter, the auditor needs to perform a particular role in Electronic Commerce payment system environments. This Chapter highlights issues in order to explain the role of the Information Systems (IS) auditor in an Electronic Commerce environment.

The aim of this chapter is firstly to provide a definition of auditing and to explain the different auditor types. The objectives of each type of audit are also highlighted. The second aim is to provide an explanation of the expectations of management regarding the work of the auditor, as well as the role of the IS auditor in new technology environments such as EC. Thirdly, this chapter highlights the audit process that an IS auditor should follow in the execution of an audit. This process also includes the involvement of the IS auditor in an EC environment.

In this chapter, the abbreviations IS (Information Systems), IT (Information Technology), and EDP (Electronic Data Processing) are used interchangeably due to their use in quotations by different authors, but effectively they refer to the same concept, which is expressed in simple terms as the computer environment. Quotations used throughout this chapter refer to these three terms, but for subsequent chapters the term IS Audit is more commonly used.

2.2 AUDITING DEFINED

In order to understand the function of audit, the following definitions are provided for Auditing:

- The American Accounting Association's definition of auditing (Vallabhaneni, 1991); (UDEL, 2002); (IUSB, 2002) is broadly applicable to several types of auditing (explained in section 2.3 below), including external auditing, internal auditing, and IS auditing: "Auditing is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions

and events; to ascertain the degree of correspondence between those assertions and established criteria; and communicating the results to interested users."

- "Auditing is the process of classifying, evaluating, and measuring the integrity of the statements, work, or possessions of others" (Menkus, 1998).
- A further definition of Audit is provided by the *World Book Encyclopaedia* (World Book, 2001) as follows: "Auditing is the systematic and official examination and check of business activities."
- The DTI Commercial Computer Security Centre as quoted by Walden (Walden & Braganza, 1993) defines an audit as: "An independent review and examination of system records and activities in order to test for adequacy of system measures, to identify the degree of conformity with established policy and operational procedures and to recommend any indicated changes in measures, policy, and/or procedures."

Concepts obtained in these definitions are further elaborated on below, especially as they pertain to IS auditing:

- Systematic process – means that auditing is structured as a dynamic activity in a logical manner. It is an important approach to auditing all types of systems, but it is particularly important in auditing computerised systems. This is difficult to do in a computerised system where the IS auditor cannot visually ascertain the processing being performed or the content of files.
- Obtaining and evaluating evidence – in obtaining and evaluating evidence, the IS auditor is concerned about the reliability of the system of internal control and the content of files produced by computer processing.
- Communicating results – the IS auditor, like all auditors, is responsible for communicating the results to interested users. Interested users in this case include other members of the audit team, external parties, and management of an organisation, depending on the type of auditor.

Auditing is therefore summarised as a systematic and independent process to examine and evaluate evidence regarding the adherence to policies and procedures, the integrity of statements, and the communication of the results.

2.3 AUDITOR TYPES

There are basically four types of auditors (Oregon University, 2001); (Wilkinson et al, 2001); (Messier, 2000), (UIS, 2001); (UDEL, 2002); (IUSB, 2002); (TEA Division of School Audits, 2002); (Bradley, 2002); (Vining 2001):

- External/Independent Auditors
- Internal Auditors
- Government Auditors
- Tax auditors (a.k.a. internal revenue agents).

Other authors (Wilson & Root, 1983); (Vallabhaneni, 1991); (Walden & Braganza, 1993) only emphasise the first two of these auditor types. This is due to the fact that the last two types mentioned are specialised and their work is limited to addressing aspects related to their specific organisations. However, many government auditors' responsibilities are the same as those of external auditors (UDEL, 2002). Due to these overlapping responsibilities, this study will focus only on the first two types.

However, it is worth noting that the role of the first two auditor types may also overlap (e.g., external auditors may conduct operational audits and internal auditors may perform financial reviews). Both internal and external auditors may perform information system audits, which support both financial and operational audits. "The explosive growth of Electronic Data Processing (EDP) has affected all the audit groups, requiring each to develop EDP audit expertise within a particular area of concentration" (Wilson & Root, 1983).

Audit firms (considered external or independent auditors) and internal audit departments are using the services of qualified computer audit specialists. IS auditors generally work closely with audit staff members, though they may not be directly involved in the non-computerised portions of the audit. The roles of the internal and external auditors are explained below, followed by a separate description of the role of the IS Auditor.

2.3.1 EXTERNAL/INDEPENDENT AUDITING

External Auditing is defined (Vallabhaneni, 1991) as:

"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."

The objectives of an independent audit is defined by the American Institute of Certified Public Accountants (AICPA) (AICPA, 1997) as "the expression of an opinion on the fairness with which they (the financial statements) represent, in all material aspects, financial position, results of operations, and its cash flow in conformity with generally accepted accounting principles". This view is also expressed by Cooper (1982). Auditors also need to adhere to certain standards (Audit Commission, 2000). 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 AICPA. There are usually similar principles and standards in use in other countries.

2.3.1.1 The Role of the External Auditor

The role of the external auditor is defined (Vallabhaneni, 1991) as follows: "The external auditor evaluates the reliability and validity of systems controls, whether manual or automatic. The principal 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 focuses on the fairness and consistency of the organisation's presentation of its financial data and provides an independent opinion about its reliability and accuracy" (Menkus, 1998). This type of audit is considered a financial audit. As far as the role of the auditor in financial audits is concerned, it is said that the purpose and scope of a financial audit is to determine whether the overall financial statements of an entity are prepared and reported in accordance with specified criteria (standards) (Companies-house, 2000); (Gilhooley, 1986). The audit scope is usually limited to accounting-related data. Financial audits are conducted by independent auditors who are "external" to the organisation being audited. External auditors express an opinion on the overall fairness of the financial statements (Audit Commission, 2000). Financial audit objectives are discussed in more detail in 2.3.1.2 below.

The role of the external auditor in a computer environment is defined as follows:

- "The auditor will need to gain an understanding of the entity's use of computers and their impact upon the financial information" (SAICA, 1998).
- Standards issued by professional organisations such as AICPA (AICPA2, 1997) describe the role of the auditor in a computer environment. As an example, the standard AU Section 8401 – Auditing in a Computer Systems Environment - states that: "The auditor should have sufficient knowledge of the Computer Information System (CIS) to plan, direct, supervise, and review the work performed." "The auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level."
- The external auditor responsible for testing the reliability of client computer systems should have a special combination of skills and experience. Such an auditor must be thoroughly familiar with the attest function (Vallabhaneni, 1991); (Wilson & Root, 1983). The attest function encompasses all activities and responsibilities associated with the rendering of an opinion on the fairness of financial statements (Vallabhaneni, 1991); (Wilson & Root, 1983). Besides the accounting and auditing skills involved in performing the attest function, these external auditors must also have substantial IT experience and training.

From the above, it is clear that external/ independent auditors have a responsibility in a computer environment as defined by the principles and standards of the professional organisations to which they belong. This role includes obtaining sufficient knowledge of the IT environment of the organisation being audited, as well as providing assurance that the IT environment is adequately controlled.

2.3.1.2 General Financial Audit Objectives

The Balance Sheet and Income Statement are two of the primary outputs of the financial reporting process. "A Balance Sheet provides the financial status of an entity at the end of an accounting period, while the income statement reports income earned during an accounting period" (Vallabhaneni, 1991).
General audit objectives for the financial audit include, according to Vallabhaneni (1991) the following:

- To evaluate whether the account balances appear reasonable in the financial statements.
- To determine whether the amounts included in the financial statements are valid.

- To determine whether all amounts that should be included have actually been included in the financial statements.
- To ensure that assets included in the financial statements are owned by the entity and that liabilities belong to the entity.
- To determine whether the amounts included in the financial statements are properly valued.
- To determine whether correct amounts are included in the correct accounts and that accounts are properly classified in financial statements.
- To determine whether transactions near the balance sheet date are recorded in the proper accounting period.
- To determine whether details in the account balance agree with related subsidiary ledger amounts, foot to the total in the account balance, and agree with the total in the general ledger.
- To ensure that all balance sheet and income statements accounts and related information are correctly disclosed in the financial statements and properly described in the body and footnotes of the statements.

The IS auditor assist the external/independent auditor in achieving these objectives in a computer environment. These objectives will then also become the objectives of the IS auditor in the role of an external auditor. The scope of the IS audit will however be limited to the computer environment.

2.3.2 INTERNAL AUDITING

Internal Auditing is an independent appraisal activity established within an organisation as a service to the organisation (Vallabhaneni, 1991); (Perry, 1988), (Walden & Braganza, 1993), (AICPA, 1997). 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) (Wilson & Root, 1983).

Internal audit is not a mandatory function within a company but the developments in the auditing and accounting fields related to internal controls (and the responsibilities of management as defined by the COSO (the Committee of Sponsoring Organisations of the Treadway Commission's Internal Control - Integrated Framework (USA)), Cadbury (UK), Co in Canada (ISACA, 1999), and the King

Commission (South Africa) etc., makes this function more desirable. Internal audit is an internal control function, including continual activities for the monitoring and testing of all IT functions. Of particular concern is the processing of data of financial relevance. Internal auditors are "internal" to the organisation being audited. Internal auditors also review financial transactions and statements but do not express an opinion to the public, while external auditors do (Wilson & Root, 1983).

2.3.2.1 The Role of the Internal Auditor

As far as the role of the Internal Auditor is concerned, the following statements are provided:

- "The purpose of the internal audit function is to assure management that authorised controls regarding the securing of company assets are being applied effectively and that the procedures allow for control to be exercised" (Oliphant, 1998).
- A further definition states that the purpose is "to assess the adequacy, effectiveness, and efficiency, of a company's system of internal control as well as quality of its ongoing operations." (Gilhooley, 1986).
- (McNamee, 1995): "The key task of the Internal Auditor is to provide unbiased information to the leaders who are trying to anticipate change. Because the organisation needs different strategies at different phases of its growth cycle, the information required by the leaders at different phases is also different. Strategies that worked well in one phase do not work well in another."
- "It is Internal Audit's role to carry out an independent appraisal and evaluation of the effectiveness of these controls. Internal Audit is not part of line management. Audit does not develop and install procedures, prepare records or engage in any activity which could compromise its independence. The emphasis on independence in no way diminishes the close working relationship and need for communication between Internal Audit and other functions of the organisation that they work for. This communication is particularly important, as Audit's role includes appraising and advising on the controls to be included in new or revised systems, both computer and manual, before they are introduced" (IC, 2000).
- "The internal auditors provide management and the board of directors, through the audit committee, with a means of monitoring the reliability and integrity of information about the company's finances and its operations. The audit

committee should expect the internal auditors to examine and evaluate the adequacy and effectiveness of the organisation's internal control structure and the quality of performance in carrying out assigned responsibilities. The internal auditors may also perform special projects for the audit committee" (Westwood, 1997).

These statements show that Internal Audit has a responsibility towards management of an organisation, and this responsibility includes an evaluation of the internal control environment. The internal control environment in turn also includes the computer environment and therefore the involvement of the IS auditor. The role of management in the control environment is highlighted in section 2.4 below.

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 (Vallabhaneni, 1991).

Internal audit services include examinations of internal controls, financial statements, standards of business conduct, operations, and EDP (Wilson & Root, 1983). "Top management must be concerned with the reliability of computer generated information upon which critical organisational decisions are made. In organisations in which management is sincerely concerned about this reliability, internal auditors are growing in stature" (Vallabhaneni, 1991).

There are various types of internal audits (WUStL, 2000); (GT, 2000); (Emory, 2000); (Wilson & Root, 1983); (UDEL, 2002); (IUSB, 2002); (Bradley, 2002); (Vining, 2001):

1. **Operational** audits are designed to "add value" to the area audited, they often consist of analyses of procedures and document flows for efficiency and necessity (WUStL, 2000). In operational audit, the auditor reviews existing operations to recommend improvements on efficiency and effectiveness (GT, 2000); (McNamee, 1995); (AICPA2, 1997); (Vallabhaneni, 1991). Operational audits review operating information and the means used to identify, measure, classify, and report such information; review the means for safeguarding assets; ascertain whether results are consistent with management's objectives and goals and whether the operations are being carried out as planned, and appraise the

economy and efficiency with which resources are employed (Emory, 2000). Operational audits are intended to help an organisation become more productive and more profitable (World Book, 2001). The scope should be broad enough to include any function in the organisation such as Electronic Data Processing (EDP), marketing, manufacturing, finance, accounting, personnel, and other areas. Operational audits are usually conducted by internal auditors and government auditors, with the latter involving financial and operational audits of government agencies.

General audit objectives for an operational review include the following (Vallabhaneni, 1991); (Perry, 1988):

- To ensure the reliability and integrity of information,
- To ensure compliance with policies, plans, procedures, laws, and regulations,
- To ensure the safeguarding of assets,
- To ensure the economical and efficient use of resources, and
- To ensure the accomplishment of established objectives and goals for operations or programs.

2. **Financial** audits are designed to validate the accuracy, completeness, and authorisation of financial transactions, records, and account balances of the audited area. These audits also include analyses of internal controls of the area and system audited (WUStL, 2000). Financial audit reviews the controls pertaining to the recording, summary and analysis of financial information (GT, 2000); (AICPA2, 1997). Financial audits address questions of accounting and reporting of financial transactions, including commitments, authorizations and receipt and disbursement of funds (Emory, 2000). (VAG, 2001). The principal purpose of a financial audit is to add credibility to the financial statements by the expression of an independent opinion thereon – this is considered to be the role of the external auditor. Financial audits check the reliability of financial information (World Book, 2001). Financial audit objectives have been mentioned in 3.1.2 above.

3. **Compliance** audits are designed to review and evaluate compliance with the institution's policies and procedures, as well as any applicable external (e.g. governmental) rules and regulations (WUStL, 2000). In compliance audit, the auditor verifies current practice against regulations laid down either by the company or external parties (GT, 2000). Compliance audits determine the degree

of adherence to laws, policies and procedures (Emory, 2000); (McNamee, 1995); (AICPA2, 1997); (World Book, 2001).

4. **IS/IT audits** will be described in more detail below.

5. **Fraud detection and investigation** audits – The purpose is to detect fraudulent activities and investigate them further.

Standards for internal audit are prescribed by the Institute of Internal Auditors (IIA), and for IS auditors in an internal audit capacity, the standards are prescribed by Information Systems Audit and Control Association (ISACA).

Audits performed by the Internal Audit Department are combinations of operational, financial, compliance and IS auditing. Fraud detection and investigation also plays an important role, and in the experience of the author, some international audit departments have established a separate fraud investigation section especially in high-risk organisations in the financial sector (e.g., banks and insurance companies). Here the IS auditor also plays an important role as the computer may be used to collect evidence.

From the above it is clear that the internal auditor has a responsibility to evaluate the controls in an IT environment. To address this responsibility, the IS auditor plays an important role through the evaluation of computer related controls.

2.3.3 INFORMATION SYSTEMS (IS) AUDITING

2.3.3.1 Introduction - IS Auditing Defined

It is necessary to review a few definitions of IS auditing to obtain a better understanding of this function.

- 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." (Vallabhaneni, 1991).

- IS auditing is any audit that encompasses the review and evaluation of any portion of automated information processing systems, including related non-automated processes, and the interfaces between them (EDP Auditors Foundation, 1994).
- IS auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organisational goals, and consumes resources efficiently (Sayana, 2002); (Pathak, 2000).
- "Information Technology (IT) audits are designed to evaluate controls surrounding computer centres, computer systems, and data input, processing, and output controls. These audits consist of specific IT audit techniques to ensure the adequacy and reliability of controls and to ensure the integrity of data processing." (WUStL, 2000).
- "EDP audit covers computer related areas such as the Year 2000 issue, backup and recovery, application system development, etc." (GT, 2000).
- "Information Systems Audits evaluate system input, output and processing controls, backup and recovery plans and system data and physical security" (Emory, 2000).

According to the above definitions IS auditing is therefore considered as the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organisational goals effectively, consumes resources efficiently, and adheres to policies, procedures, standards, rules, laws, and regulations. This evaluation may include the assessment of how efficient, effective, and economical computer based practices are. The evaluation should also determine the adequacy of internal controls within the IT environment to assure valid, reliable, and secure information services.

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 may be visualised as something that helps organisations to better attain these objectives.

Information Systems auditing refers to auditing performed in the computer environment. An IS audit environment means either or both of the following:

- The evidence that the auditor gathers, originates, or is maintained in a computer system.
- The auditor uses computer-based techniques to gather or evaluate evidence.

"The information systems (IS) audit is not a stand-alone activity" (Vallabhaneni, 1991). It is an integral part of the external or internal auditing function. Information systems audits deal with reviews of computer operations and application systems where computer equipment is located and computer-based systems are used.

The 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 ISACA, the Information Systems Audit and Control Association. 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 (Wilson & Root, 1983)).

It is important for IS 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 as provided by ISACA. As a guideline for IS Audit, ISACA developed the 'Control Objectives for Information and related Technology (COBIT) Framework. The main objective of COBIT is "the development of clear policies and good practices for security and control of IT" (ISACA, 1999).

The following definition (based on the concepts promulgated in "Internal Control – Integrated Framework" developed by COSO) may be considered as the mission of IS Auditing (Paliotta, 1999). "Using appropriate technological tools and expertise, evaluate the adequacy and effectiveness of control systems addressed to the risks emanating from an organisation's application of technology in support of its business objectives and proactively work with management to identify risks and control objectives in the application of emerging technologies in support of strategic objectives."

The role of the IS auditor is therefore regarded as evaluating the controls in the IS environment as part of their responsibility to management of the organisation and other interested parties. This role may either be performed in the capacity of an external or an internal auditor.

2.3.3.2 Information Systems Audit Control Objectives

There are several detailed information systems control objectives that an internal control structure must meet. They must be able to prevent, detect, and correct errors, omissions, irregularities, and computer intrusions such as viruses and worms, and to recover from such activities to assure continuity of business operations. Here, the term "system" includes hardware, data, software, people, documentation, and the associated procedures, whether manual or automated.

These control objectives are also embedded in the COBIT framework and include (ISACA, 1999); (Vallabhaneni, 1991):

- System assets are safeguarded. An organisation's information technology assets and resources such as computer facilities, computer equipment, people, programs, and data, are to be safeguarded at all times to minimise waste and loss (Gilhooley, 1990).
- System reliability is assured. The objective is to ensure that the hardware, software, and data are stable, and that people can be trusted to carry out the organisation's mission.
- Data integrity is maintained. This deals with controls over how data is entered, communicated, processed, stored, and reported. The objective is to ensure that the data are authorised, complete, accurate, consistent, and timely.
- System security is assured. An organisation's assets and information resources are to be protected from unauthorised access and use.
- System availability is assured. The objective is to ensure that the system (hardware, software, and data) and its components are available when they are needed, where they are needed, and to those who need it.
- System controllability is maintained. Adequate manual and automated controls and procedures over hardware, software, data, and people should be available.
- System maintainability is assured. The system, excluding hardware and software, should be maintained with existing resources at minimum cost and time.

- System usability is assured. For example, the application system is appropriately user-friendly, or the system design invites rather than inhibits the authorised user to use it.
- System effectiveness is ensured. For example, system effectiveness is measured by determining whether the system performs the intended functions and that users get the information they need, in the right form, and in a timely fashion.
- System economy and efficiency are maintained. An economical and efficient system uses the minimum number of information resources to achieve the output level the system's users require. Economy and efficiency must always be considered in the context of system effectiveness. The system must promote operational efficiency (Gilhooley, 1990).
- System quality is maintained. This is an overall goal. In addition to the above, the computer system should have built in quality-related features such as testability, portability, convertibility, modifiability, readability, reliability, consistency, understandability, and adequate documentation.
- System must encourage compliance with managerial and fiduciary laws, policies and regulations (Gilhooley, 1990).

The purpose and scope of information systems audits are to determine whether controls over computer systems and information technology assets are adequate. These particular types of audits are conducted by IS auditors, who may be external or internal to the organisation being audited (Vallabhaneni, 1991).

The above objectives include control over EC payment security and the IS auditor should apply these control objectives, if applicable, as part of the process to develop an audit approach for the audit of EC payment security.

2.3.3.3 Information Systems Audit Objectives

The audit objectives (related to the control objectives mentioned above) of information systems audit are to:

- Ensure that adequate audit coverage of major risks and exposures in an IT environment is available.

- Ensure that IT resources are allocated to computer hardware, peripheral equipment, software, services, and personnel in an efficient and effective manner to achieve the IT department's and organisation's goals and objectives.
- Provide reasonable assurance that computer related assets (e.g. data, programs, facilities, equipment, supplies) are safeguarded.
- Ensure that information is timely, accurate, available, and reliable.
- Provide reasonable assurance that all errors, omissions, and irregularities are prevented, detected, corrected, and reported.
- Obtain the most efficient usage of audit resources (staff, time, and money).

The above objectives therefore include an evaluation of the controls in any environment, which include the Internet, and therefore EC payment security.

The IS auditor is therefore considered as someone who performs an essential role in the capacity of an external or internal auditor, and has the responsibility to evaluate the control environment in an organisation where IT is used. This role is also an essential function to assist management of an organisation as described in section 2.4 below.

2.4 IS AUDIT AND MANAGEMENT EXPECTATIONS

Executive management's focus on information technology varies dramatically depending on the mission of the organisation, the industry, the culture, and whether technology is a product or service provided or consumed by the organisation. The auditor's role within an organisation may also vary greatly depending on executive management expectations of audit and the state of controls within the organisation. In general, management expects auditors to assess controls, rather than define or prescribe them. Management should also regard information as a major organisation asset, the protection of which must preoccupy all executive managers.

Senior management has a responsibility to establish effective control over information and information systems (CICA, 1986); (ISACA, 1999); (Menkus, 1998). Discharge of this responsibility involves the exercise of management practices, which are as applicable to information systems as they are to other activities of the entity, and is summarised as follows (CICA, 1986); (Oliphant, 1998):

- Establishment of objectives and policies for each role and function.
- Assignment of the related responsibilities.
- Development of a comprehensive plan for the achievement of the information system's objectives and policies for the entity.
- Monitoring of activities against the company objectives, policies, and plans.

The following statements defines the responsibility of control:

- The directors should report on the maintenance of an effective system of internal controls. This is a requirement of the King report on Corporate Governance in South Africa.
- Ensuring the integrity of the corporation's accounting and financial reporting systems, including appropriate systems of control (OECD, 1999).
- It is the responsibility of the audited body (Audit Commission, 2000) to:
  - Put in place proper arrangements to ensure the proper conduct of its financial affairs, and to monitor their adequacy and effectiveness in practice.
  - Develop and implement systems of internal control, including systems of internal financial control and to put in place proper arrangements to monitor their adequacy and effectiveness in practice.
  - Ensure its affairs are in accordance with proper standards of financial conduct and to prevent and detect fraud and corruption.
- Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance and/or operation of information systems (ISACA, 1999).
- Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. According to ISACA (1999):

  "Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide. Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources."

- "Control of information systems is the responsibility of senior management" (CICA, 1986). The inherent partnership between auditors and management requires that the auditors understand management's concerns, ensuring that the organisation's structure addresses business objectives including:
  - Quality of the organisation's products and services
  - Customer and business partner satisfaction
  - Cost management, revenue/profit maximisation, and effective and efficient operations
  - Information management for integrity, availability and privacy
  - Safeguarding of assets including information assets
  - Regulatory and internal compliance
  - Business continuity
  - Fraud prevention and detection
  - Technology innovation appropriate to the organisation's objectives
  - Accurate and timely financial reporting.

From these statements, the responsibility of the IS auditor is defined as to consider the activities and assets that would interest a third-party stakeholder or management in the organisation – one who understands IT issues, opportunities, and potential problem areas, and who has a strong interest in the organisation's performance. The auditor must then develop an understanding with executive management about the relevance of each of these areas, with some measure of their importance or potential risk, comprehending the degree of technical complexity involved in assessing them and providing audit results.

The responsibilities of the internal and external auditor towards management and external parties respectively are defined by Wilson and Root (1983) as: "Internal auditors provide boards of directors and companies' management with assurance as to the sufficiency of the authorised control techniques to accomplish business goals and the degree of compliance therewith." External auditors "provide assurance to stockholders, creditors and others regarding the fairness of the information contained in the financial statements."

The ICAEW's booklet (GT, 2000) on "Internal Audit and its Value" highlights 3 areas in which internal audit assist management of organisations, namely:

1. Meet their corporate governance responsibilities.

2. Assess and manage business risk.
3. Ensure adequate systems of internal controls.

According to Miller (1999):

> "Stakeholders expect Internal Auditors to ensure that the organisation's assets are safeguarded. This extends to critical information security. The Internal auditor may well be the person with the broadest perspectives and knowledge base when it comes to understanding the control environment and the control systems that provide infrastructure protection. For the current audit evolution to be complete, Internal Auditors must recognise the elements of information security as key in providing reliable evidence about infrastructure protection and assurance."

The following statements further highlight the relationship between IS audit and management:

- "Nobody understands the changing audit environment better than IS auditors who deal with new and emerging technologies and objectives and techniques that did not exist the day before" (Garitte, 1998).
- Garitte (1998) is also of the opinion that. "Auditors should address management as experts in neither technology nor controls, but as business strategists who are keenly aware of the organisation's dependence on information, technology, and the controls that assure integrity. Auditors apply their expertise to provide the assurances management needs in terms of the integrity of information assets"
- According to Sayana (2002): "Information systems are the livelihood of any large business. As in years past, computer systems do not merely record business transactions, but actually drive the key business processes of the enterprise. In such a scenario, senior management and business managers do have concerns about information systems. The purpose of the IS audit is to provide feedback, assurances and suggestions."
- "In taking responsibility for internal controls, management must also take responsibility for IS controls. While management may be familiar with some technologies, their knowledge is short lived due to the constant change of systems. This should result in greater reliance of management on IS audit and control professionals" (Owen, 1994).

From the above it is clear that executive management therefore need not understand technical language or the details of technical tasks performed by auditors. Auditors, however, must understand management's perspectives and keep management aware of key technology issues. In short, auditors must show understanding of the significant business issues and the technology components that support them, and gather supporting evidence.

The Australian Guidance Statement number AGS1056 from the Australian Accounting Research Foundation (AARF) (2000) states that: "Management is responsible for developing an e-com strategy to address risks and opportunities arising from its e-com activities." "Ordinarily management will identify e-com business risks, and will address those risks through the implementation of appropriate security and internal control measures. The auditor considers e-com business risks in so far as they impact on audit risk."

In summary, auditors must also ensure that appropriate audit resources are applied to those issues that concern executive management. They must bring new information, positive or negative, to management's attention in such a way that management will understand its importance and act appropriately.

From the above it is clear that technology brings risks along with its potential rewards, and IS auditing also has a responsibility to increase awareness of technological risk and control issues. The IS auditors should help to educate the rest of the organisation regarding these risks in order to assure that the implementation of new technologies will achieve the corporate objectives without placing the organisation in an unacceptable risk position.

2.5 THE CHANGING IS AUDIT ENVIRONMENT AND AUDIT OBJECTIVES

The development of EC brings new challenges to the IS auditor due to the change in the way that business is conducted (e.g., a move towards a paperless environment). The complexity of audit activities varies with the complexity of the processing system; thus, the extent of required computer proficiency varies, too. The availability of visible audit evidence that may be subjected to compliance testing or substantive testing

and the planned audit approach also affects the auditor's need for proficiency in computers. Apart from the requirements from professional bodies or organisations, there are also certain expectations from management for IS Auditing.

If an audit involves computer-maintained accounting records, the auditor must have sufficient competence in IT systems to conduct the audit properly. This requirement follows from the general requirement for "adequate technical training and proficiency as an auditor", defined by the generally accepted auditing standards and rules of conduct (an example of such standard is found in the AICPA General Standards ET Section 201); (AICPA3, 1997). The first general standard (Vallabhaneni, 1991) states: "the examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor."

In an increasingly computerised and borderless environment, Internal auditors (IA) must utilise new technologies to assist companies in identifying new threats and opportunities in e-commerce, etc. (GT, 2000). The IS auditor requires new levels of skill in order to effectively audit today's complex and varied systems. The auditor must be proficient in a wide range of hardware and software systems, and audit planning techniques (Hickman, 1996).

According to Gallegos (Gallegos & Bieber, 1987) "Auditors must understand the basics of emerging technologies and must develop new audit tools and techniques." "...increased systems complexity will require that the auditor have a specialized knowledge of computer-based information systems."

As technology evolves, the auditor is required to anticipate the efforts that the directions in IT may have on business objectives (Ramos, 2001).

"If managers, information system specialists and auditors are indeed going to be able to effectively fulfill their roles, their skills must evolve as rapidly as the technology and the environment" (ISACA, 1999). Auditors must understand the technology of controls involved and its changing nature to exercise reasonable and prudent judgements in evaluating control practices found in businesses (ISACA, 1999); (Wilson & Root, 1983).

From the above statements it is clear that the auditor needs to understand new technology and to continually update their skills to keep up with changes in

information technology. The new information technology includes the EC environment. Because the IS auditor is mainly involved in the evaluation of computer related controls, this requirement to update skills and understand the new technology specifically applies to the IS auditor.

2.5.1 Auditors in an EC Environment

The various facets of the role of auditors in EC are illustrated in the following statements.

- "Many auditors today pride themselves on their expertise in internal controls. For a growing number this expertise is oriented towards controls in information systems and technology. However, highly technical, complex and esoteric systems and processes provide an increasing percentage of the fundamental controls in EC environments. Individuals (including auditors) who are capable of understanding the elements of control in such environments and who also understand the business, legal, financial, and other implications of such controls are rare indeed" (Marks, 1998).
- "Electronic commerce technologies are rapidly changing the business world, as well as the rules and conditions under which business is transacted. Accordingly, auditors must be aware of how technology impacts their business, their industry and related industries, the legal and regulatory environment, and their profession" (Marcella, 1998).
- Marks (1998) also believes that: "There are no simple audit solutions. Fortunately, the same organisations that build and use the technologies, and the technologies themselves, should solve the problem of how to provide assurances in an environment of constant change."
- The internal auditor must participate in all aspects of IT to ensure that the company's assets are being protected and that suitable internal controls are in place to protect its information resources (Oliphant, 1998). "Auditors must understand the basics of emerging technologies" (Gallegos & Bieber, 1987).
- "The widespread use and ongoing development of EC systems challenge the audit profession to examine its processes and procedures" (Stein et al, 2001). "IS auditors should therefore possess a high level of Information Technology (IT) expertise in their respective organisations. IS auditors should possess the

greatest knowledge concerning how IT may affect the audit process." (Stein et al, 2001).

- The rapid developments in the world of IT "require that computer auditors be constantly updating their skills and technical knowledge" (Oliphant, 1998). The IS auditor will constantly be faced with new challenges as newer, emerging technologies are implemented.
- According to Paliotta (2001):

  "…auditors should utilise the COSO Integrated Framework of Internal Control to expand their partnership role in the evolution of e-commerce. In particular COSO states that:

  Management is ultimately responsible for the internal control structure and should assume ownership of the system of internal controls.

  In addition to the control environment, control activities, and ongoing monitoring, the components of internal control include:

  - Risk assessment including the "identification and analysis of relevant risks to the achievement of objectives"
  - Information and communication, including "information about external events, activities and conditions necessary to informed business decision-making and external reporting"

  Consequently, the audit strategy should be expanded to include raising management's and the board of directors' awareness of the significance of protection and security of information relative to e-commerce plans and the attendant risks that could jeopardise those plans."

Executive management therefore needs assurance from the organisation's auditors, both internal and external, that appropriate assessments have been performed, and that any problems or concerns receive appropriate attention. They must be able to depend on auditors to explain the value of the organisation's information assets, and to have the technical competence to address the processes, systems and technologies that protect information and maintain its value. IS auditors are also expected to understand how trends and innovations in technology will impact on the organisation, and to adjust the audit approach, practices and objectives accordingly to ensure that auditing remains relevant and useful to the organisation and its management. Standards for professional audit practices provide the requirement for and govern the practices of auditors providing such assurances. The standards will be highlighted further in 2.5.2 below.

From the above statements it is clear that IS auditors should therefore perform the following with respect to advances in new technology:

- Keep up to date with leading edge technologies being considered to support and enable business operations.
- Obtain an understanding of how new technology will relate to the business process.

The IS auditors therefore have a responsibility to understand new technology and therefore need to update their skills continuously. This understanding is essential for the IS auditor to be able to fulfill his duty/ obligations towards management and other interested parties in an organisation. This responsibility is also defined by the professional organisation's standards for auditors and accountants.

2.5.2 Audit Guidance in Electronic Commerce Environments

In order to provide guidance to the IS Auditor in complex technical environments (such as EC) and to fulfill the IS Auditor responsibility to management, several developments in the audit field have taken place. These include the developments mentioned in sections 2.5.2.1 to 2.5.2.3 below.

2.5.2.1 Audit Guidance Statement – AGS1056

"The Australian Board is the first worldwide standard setting body to develop authoritative guidance to address emerging audit issues in the new business environment of Electronic Commerce (EC)" (Lymer, 2000).
The Australian standard (Australian Accounting Research Foundation (AARF) (2000) - AUS 304 - "Knowledge of the Business") requires that "the auditor obtain knowledge of the business sufficient to enable the auditor to identify and understand the events, transactions and practices that may have a significant effect on the financial report or on the audit report." "Knowledge of the business includes a general knowledge of the economy and the industry within which the entity operates" (AUS 304.03). The growth of EC may have a significant impact on the entity's traditional business environment.

It is further stated (AARF, 2000) that:

The auditor's knowledge of the business is fundamental to assessing the significance of EC to the entity's business activities and any impact on audit risk. The auditor requires appropriate IT skills and Internet knowledge to be able to make appropriate inquiries to:

- Understand the business;
- Understand the entity's business strategy, and particularly the EC strategy and EC business model;
- Understand the technology;
- Assess the IT skills and knowledge of entity personnel.

The auditor obtains knowledge of the entity's EC activity with regard to changes in the business environment attributable to EC and the EC business risks as identified.

2.5.2.2 Web Assurance Framework

The American Institute of Certified Public Accountants (AICPA) (1999) and the Canadian Institute of Chartered Accountants (CICA) joined forces to develop and offer an electronic commerce (EC) assurance service. Accounting firms that are duly licensed by the AICPA or CICA may provide assurance services to clients and place the WebTrust seal of assurance on their clients' World Wide Web sites. Users who engage in EC with a company that displays the seal are provided with certain assurances regarding compliance with disclosed business practices, integrity of EC transactions, and protection of private information.

According to the AICPA and CICA (AICPA, 1999):

> 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.

2.5.2.3 Audit standards

Standards issued by professional organisations such as AICPA (1997) describe the role of the auditor in a computer environment. As an example, the standards issued by the AICPA include:

AU Section 8401 – Auditing in a Computer Systems Environment. "The auditor should have sufficient knowledge of the Computer Information System (CIS) to plan, direct, supervise, and review the work performed." "The auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level."

Standard number 040.010 of the ISACA regarding skills and knowledge states (ISACA, 2001): "The IS auditor is to be technically competent, having the skills and knowledge necessary to perform the auditor's work."

The audit and accounting guide issued by the South African Institute of Chartered Accountants (SAICA) contains the following statement: "The auditor will need to gain an understanding of the entity's use of computers and their impact upon the financial information" (SAICA, 1998).

According to the above statements, in order to obtain or update knowledge of the entity's e-commerce activity sufficient to enable the auditor to identify and understand the events, transactions and practices that may have a significant effect on the financial report or on the audit or the audit report, the auditor considers various aspects of the entity's EC activity and the industry in which it operates, including:

- The entity's awareness of business risks.
- Whether management has addressed security issues.

The EC environment should therefore be treated in the same way as any new technology. The EC environment is developing at a rapid pace and the guidance from the professional organisations is therefore limited. The IS auditor still needs to

understand this new technology. This understanding will enable the IS auditor to perform an audit in this new technology by following the audit process highlighted below.

2.6 THE AUDIT PROCESS

The following steps have been defined as the audit process to be followed when conducting an audit. These steps have been defined by the Information Systems Audit and Control Association (ISACA) in the CISA review manual (CISA, 2001); (Perry, 1983); as well as other professional organisations (e.g., the South African Institute of Chartered Accountants (SAICA), (SAICA, 1998 – first 4 steps (numbered points below)):

1. The preparation before an audit involves collecting background information and assessing the resources and skills required to perform the audit (Sayana, 2002). This background information gathering process in the EC environment is addressed in Chapter 3 of this study.
2. Risk assessment – This step is addressed in Chapter 4 of this study.
3. Controls identification - This step is addressed in Chapter 5 of this study.
4. Audit approach formulation – this is the ultimate objective of this study and is addressed in Chapter 6 of this study.
5. Testing of controls.
6. Reporting on results.
7. Follow up on outstanding issues.

As stated above, as well as in Chapter 1 of this study, the ultimate goal of this study is to formulate an audit approach and the last 3 steps are therefore not included in the remaining chapters.

2.7 CONCLUSION

This chapter identified the various types of auditors and highlighted the objectives of the auditors including the objectives of the IS auditor. The role of the IS auditor involves the evaluation of the controls in the IS environment as part of their responsibility to management of the organisation and other interested parties. This role also includes understanding the IT environment (including computer jargon and

technologies), identifying weaknesses and risks, and adding assurances to management and other interested parties. The role of the IS auditor is defined either in the capacity of an external or an internal auditor.

This chapter also showed that auditors must also ensure that appropriate audit resources are applied to those issues that concern executive management. They must bring new information, positive or negative, to management's attention in such a way that management will understand its importance and act appropriately.

Electronic commerce is a broad and varied field prone to technical complexity. Understanding and assessing controls in this environment force IS auditors to continuously update their skills and to provide management of an organisation with assurance on the control environment for this new technology. This chapter also showed that the IS auditors need to adhere to the standards of the professional organisations that they belong to. These standards also require the IS auditor to keep their skills and knowledge up to date with changes in the IT environment. It was highlighted that there have been developments in the audit area that provide guidance to the IS auditor in an EC environment.

This chapter finally highlighted the audit process to be followed by IS auditors. This audit process is also applicable to the EC environment and therefore the audit of EC payment system security. This process will be explained in more detail in the ensuing chapters of this study and the end result will be the identification of an audit approach to be followed by the IS auditor in the audit of EC payment security.

CHAPTER 3

ELECTRONIC COMMERCE AND ELECTRONIC COMMERCE PAYMENTS

INDEX

3.1 INTRODUCTION.

The objective of this dissertation is the development of an audit approach directed at Internet payment security. An explanation of the relevant concepts related to Internet payment security and electronic commerce is therefore necessary. This chapter will provide a background to electronic commerce and will include the aspects of electronic commerce related to Internet payments. This background is essential to the IS auditor so that a complete understanding of the issues involved will be obtained and so that the importance of electronic commerce will be highlighted. The IS auditor has an important role to play in electronic commerce payment systems. This understanding will then aid the subsequent risk and control identification process. The concepts of risks and controls are introduced in this chapter, and dealt with in detail in Chapters Four and Five, focusing on the risks and controls of electronic payments over the Internet.

"In just a few short years, the Internet has expanded from a limited access academic and research network into a universal, multipurpose electronic medium" (Choi et al, 1999). This aspect will be highlighted in section 3.2.1 below. "In addition to educational and research uses, it has become a popular medium of choice for communicating, advertising and, with the advent of the World Wide Web, for doing business" (Choi et al, 1999). According to PWC (PWCglobal, 1999), "... e-business is the future. It is redefining commerce, transforming industries, and eliminating the constraints of time and distance". This view is also emphasised by the OECD report (OECD, 1999).

Electronic commerce enables businesses to innovate processes from production to customer service by integrating them in a seamless whole. Consumers may search and order products online, exchange product information, learn about product quality from other online users, and negotiate with sellers for lower prices and better quality. Governments are developing electronic commerce platforms to collect taxes, disseminate information, monitor market processes and interact with citizens via personalized, up-to-date communications networks.

According to Choi (Choi et al, 1999) "Electronic commerce has far-reaching implications for the future economy due to the heightened interest among businesses, researchers and government policy makers. Journalists and magazine

columnists are making more money on the Internet than are many businesses." Section 3.2.1 below will provide statistics of the success stories related to Internet business. This chapter focuses on electronic commerce and the development of this technology. It is necessary to understand the technology and the aspects around e-commerce so that the background obtained will aid in the identification of the risks and controls involved. This chapter also includes an introduction to electronic commerce payments and a short introduction to risks and control mechanisms around such payments. The risks and controls surrounding e-commerce payments will be discussed in more detail in subsequent chapters.

3.2 ELECTRONIC COMMERCE

3.2.1 ELECTRONIC COMMERCE DEFINED

Electronic Commerce is defined (Cobb, 1998) as "The use of computer networks – the Internet, intranets, extranets, and private networks – to complete business transactions."

Another definition (Martin, 2000) states: "Electronic commerce includes all commercial activities performed through various electronic sources such as the Internet, IT networks, ATM machines, EFT, and EDI, and one of its distinct characteristics is the use of computer to perform the transactions". ISACA (2000) defines e-commerce as "the processes by which organisations can conduct business electronically with their customers, suppliers, and other business partners, using the Internet as an enabling technology". This "does not include existing non-Internet E-commerce methods based on private networks, such as EDI and S.W.I.F.T."

The issues involved in Internet commerce affect large and small companies. As of January, 1996, "half of all businesses with more than 1,000 employees had at least one Web site, according to a Yankee Group survey (which also found that nearly two thirds of all companies with web sites had less than 100 employees)" (Cobb, 1999).

These definitions show that EC basically involves the use of computers to conduct business electronically. This process includes Internet payments, which is the focus of this paper.

To highlight a few examples of the sales of goods and services over the Internet, the US Department of Commerce (1998) quoted the following statistics:

- By the end of 1997, 10 million people in the U.S. and Canada had purchased something on the Web, up from 7.4 million six months earlier.
- 1-800-Flowers sold $30 million online in 1997. While this represents only 10 percent of the company's total revenues, its profit contribution to the overall business is nearly that of its store based business, which is twice as large.
- Amazon.com offers a selection of 2 million book titles to Internet customers (traditional bookstores have about 150,000 titles). In 1996, the company recorded sales of less than $16 million. In 1997, its sales reached $148 million.

This does not only apply to the USA. According to Liang (1999), "...electronic commerce also grows rapidly in Western European countries". Germany Britain and France were identified as "the top three consumer online markets in Europe" and "electronic commerce is also growing rapidly in Australia". "In Asia, although Electronic Commerce revenues are still small compared to the US, it is growing fast".

This view from Liang is also shared by the 1999 OECD report.

The Internet may be attractive to smaller companies because it enables them to reach a wide audience/market with a presence that could be as impressive as that created by much larger entities. According to Cobb, "most major corporations see enough potential to invest significant dollars (over $500,000 per company in the 1,000 employee plus category)." These statistics show that the business over the Internet has experienced phenomenal growth over the past few years. The expectation is that this growth will continue. This highlights the fact that e-commerce is an important factor in business, and the IS auditor must familiarise him/herself with the concepts of e-commerce.

3.2.2 THE HISTORY OF ELECTRONIC COMMERCE (EC)

The following is a brief description of the development of EC according to PWC (1998).

> "Prior to 1997 Web-based EC was not used extensively. There was uncertainty about which products and services should be used to develop commerce sites, to provide Web-enabled content such as advertising or publishing, or to support business activities such as sales or customer service. EC was identified mainly with electronic data interchange (EDI) - an older, less flexible technology that seemed out of step with the new ways of doing business electronically via the Internet."

The use of EDI in the 1980's and early 1990's is also emphasised by EM (1993), as well as ecommerceabout (2000). The further development in the late 1990's (PWC, 1998) was as follows:

> "In 1998, the concept of EC has begun to crystallise in the thinking of most businesspeople. EC enabling tools and technologies – for example, products and services for site development and operations – are recognised as a multi-billion dollar industry in their own right. Perhaps more important, EC is now understood to include the customer interactions of advertising, product selection, contract negotiation, and so on – all the way through to the product and service delivery phase, including logistics, payment, settlement and clearance. As the scope of EC's definition has expanded, the technologies that support EC have expanded as well. The term electronic business was introduced, which includes not only EC but all Web-enabled core business processes, extensive customer integration and connectivity, and strategic transformation of business processes to exploit the efficiencies these technologies make possible."

For many companies, Internet commerce means taking credit card orders from customers or shopping for electronic catalogs on the World Wide Web (ECA, 2000). For others Internet commerce may mean dealing electronically with clients and suppliers, as an alternative to private, leased-line electronic document interchange (EDI over Value Added Networks or VANs). This use of the Internet is sometimes called a Virtual Private Network (VPN) or tunneling. Another area of Internet commerce, which overlaps the two others mentioned here, is digital authentication (of anything from contracts and invoices to photographs).

There are many success stories related to companies that changed their businesses to include electronic commerce activities. These accounts highlight the dramatic growth of Internet business. It also shows that EC has become a very important issue that cannot be ignored by the IS auditor. IS auditors need to understand the concepts and importance of EC so that they will be able to identify the risks associated with conducting business over the Internet, and ensure that these risks are minimised through the introduction of appropriate controls in the business environment.

A few examples have been highlighted in Chapter 1. Below are more examples provided to highlight the importance of EC in business today. According to PWC (1998):

> "Consumer to business Web sites such as Amazon.com and Travelocity.com have attracted extensive media attention as they reach out to a global market, while other chains claim less attention but achieve success: The Disney Store, for example, already sells as much merchandise online as eight physical stores combined. Likewise, Internet portals such as Excite, Yahoo!, and others supported by advertising revenue have experienced rapid and dramatic growth. Through these portals, consumers may shop simultaneously for almost any category of product across many different companies, presenting a radical alternative to mail-order shopping from retailer-specific catalogs or to mall shopping full of stores with unrelated products. However, the majority of investments in technology and most of the transactions occurring over both public and private networks fall into business-to-business category. Firms such as Cisco, Compaq, and National Semiconductor now conduct a significant portion of their business over the Internet."

According to the Organisation for Economic Co-operation and Development (OECD) (1998):

> "The United States is typically credited with about four-fifths of world-wide e-commerce activity. The figures suggest that Western Europe represent about 10 per cent and Asia about 5 per cent of the world total. In Europe, the United Kingdom and the Nordic countries are the current leaders, although some estimates attribute significant activity to Germany. A supporting indicator is the location of the top 100 Web sites for consumer (retail) activity. For each of the major categories of e-commerce activities – live audio, shopping, finance,

and content (news, sports, adult) – the United States typically has 67 to 85 of the top 100 sites. Canada comes in second for five out of the six categories. Another proxy is the number of adults who access the Internet; the United States accounts for more than half".

Another aspect of EC is electronic 'communities of interest'. The goal of these is supporting and aligning similar organisations in industries such as automobiles, petroleum services, government, and health care. Other communities are also developing that focus on specific business functions, such as purchasing, payments, and human resources, or on personal interests such as investments, books, and travel.

As the above examples illustrate, EC is an aspect that cannot be ignored in today's business world. The indications are that it will grow much bigger than the current situation. It is therefore important for the IS auditor to understand the term EC and to understand what it entails. This is necessary to be able to identify the risks and the role that the IS auditor should play to ensure those risks are controlled by businesses. The next section will explain the various EC categories in the marketplace, and thereafter the two important categories will be examined in more detail.

3.2.3 ELECTRONIC COMMERCE IN THE MARKET

A market consists of (1) market agents including sellers, buyers, intermediaries and other third parties; (2) commodities and services to be exchanged, and (3) market processes such as product selection, consumer searches, competition, marketing and market research, advertising, distribution, payments and consumption. Van der Walt (Van der Walt et al, 1997) also highlights this aspect. In physical markets, consumers visit physical stores, examine products, negotiate, pay and consume physical products. Sellers send out advertisements, collect demand information through various means such as opinion surveys, and distribute their products through wholesalers and retail stores.

In the electronic market, the same market players are engaged in the same economic activities. However, they assume online identities, set up virtual firms and Web stores, communicate, search, advertise and settle payments electronically. The processes of tracking sales, collecting customer information and engineering product

specifications not only occur simultaneously, but are integrated to allow real-time feedback. According to OECD (1998) "e-commerce over open networks is a marketplace in which all types of buyers and sellers can interact".

Microproducts and micropayments allow consumers to try out products before paying for a long-term subscription or a large collection. Online usage monitoring along with micropayments enable selling a news report or a magazine column individually but also distributing copyright payments equitably and efficiently. "The electronic marketplace is very similar to physical markets in terms of the economic functions they carry out, but these market innovations can affect the structure of the market and its competitiveness." (Choi et al, 1999). In section 3.2.5 below, the different payment systems are discussed in more detail.

This shows that the basic aspects regarding trading do not change in an EC environment. The difference between 'traditional' business and EC lies in the media used to conduct the business. The underlying technology used in EC changes certain issues and especially in the areas of risks and controls. The risks and controls will be described in subsequent chapters.

3.2.4 ELECTRONIC COMMERCE CATEGORIES

According to PWC (1998): "To succeed, commerce sites targeting consumers need to offer convenience, control, and selection while saving both time and money. Business users have similar needs, but other factors may determine a site's use and success – for example, contractual terms and conditions, availability, or settlement and fulfillment options." The range of EC categories are identified as follows:

- Business to Business (B2B) EC – The use of private networks or the Internet to automate business transactions between companies (PWC, 1998).
- Business to Consumer (B2C) EC – The use of the Internet to sell merchandise or provide services to customers in much the same way as a store or a catalog (PWC 1998).
- Consumer to Consumer EC – Consumers trade amongst themselves with the website offering support and services e.g. online auctions (Hinton, 2000).
- Business to administration (government) EC -- e.g. tax and custom duty, and government and procurement purposes (Liang, 1999).

- Consumer to Administration (government) EC – e.g. welfare payments and personal income tax assessments (Liang, 1999).

The first 4 categories mentioned above are also emphasised by Steinfeld (2000), Ecommerceabout (2001), the European Commission (2000), and Strategis (2001). According to Concord (2000) - "e-commerce refers only to business-to-consumer (B2C) and business-to-business (B2B) selling over the Internet". The differences in these categories are less apparent at the level of the underlying technologies.

It therefore becomes clear that the most common categories being used today are the B2C and B2B categories. The importance of these two categories is also emphasised by Steinfeld (2000), Ecommerceabout (2001), Southcentre (2000), Ecommerce merchant accounts (1999) and Strategis (2001). It is also in these two categories where electronic payments play an important role as a transaction involving buying and selling needs to be completed with a payment. For the purposes of this research, this dissertation will therefore only focus on the first two categories where the focus is on e-commerce payments. B2B and B2C are discussed in more detail below.

3.2.4.1 B2C and B2B EC Categories

Electronic commerce is a very versatile phrase that describes a wide range of activities. It commonly refers to the following (PWC, 1998); (Liang, 1999); (Concord, 2000); (Ecommerceabout, 2001) and (Neiger, 2000):

- searching for product information;
- ordering products;
- paying for goods and services; and
- providing online customer service.

These are commonly referred to as business-to-consumer (B2C) activities.

In addition to these B2C interactions, there are also activities commonly referred to as business-to-business (B2B) activities in electronic commerce. These include

- internal electronic mail and messaging;

- online publishing of corporate documents;
- online searches for documents, projects and peer knowledge;
- distributing critical and timely information to employees;
- managing corporate finance and personnel systems;
- manufacturing logistics management;
- supply chain management for inventory, distribution and warehousing;
- sending order processing information/reports to suppliers and customers;
- tracking orders and shipments;
- making payments.

These activities for B2C and B2B will be discussed again later in this chapter. These online activities are possible because of the enabling technologies which include computer hardware, software, telecommunications networks, and products and processes such as network protocols, encryption programs, real-time applications, digital currency, cyber communities as well as digitized contents available online. According to Choi (Choi et al, 1999), "these enabling technologies are considered to be the building blocks of electronic commerce."

3.2.4.2 B2B Electronic Commerce

Business to business (B2B) EC is divided into several categories. The main ones are

- EDI, in its traditional and web-based forms;
- 'buy-side' procurement applications or systems designed to automate corporate purchasing, particularly for routine, low-value transactions; and
- 'sell-side' catalog-based sites, which in some cases include complex configuration mechanisms to allow customers to configure and price larger, high-ticket orders.

Prior to conducting transactions in the B2B venue, the buyer and the seller typically establish a contractual relationship with each other. This process differs from B2C EC, where a consumer buys from a Web site just by providing a credit-card number. Also, under the current B2B model, the seller usually extends credit to the buyer. The overall effect of the Internet on changes in businesses may also result in changes to the way transactions are initiated and flow through an organisation.

B2B EC activity is typically initiated via a purchase order, a business form (either paper or electronic) that becomes the basis for linking the various processes and stages of the transaction life cycle in both the buyer' and seller's computer systems. The stages of the transaction, linked by means of the purchase order, include origination and processing of the order, delivery, receipt, invoicing, payment, and the related financial recording.

B2B EC products often include (PWC, 1998) "features such as specialised product indexes, parametric searching by product characteristics, and the ability for a purchasing agent to download a catalog for offline searching. These products also support order and billing processes that include customised pricing and the use of purchase orders because most commercial customers buy at negotiated prices and payment terms."

3.2.4.3 B2C Electronic Commerce

According to Neiger (2000) "the most common form of e-commerce is B2C". Prior to EC, there were three B2C models (PWC, 1998): retail stores, direct sales, and mail or phone order (plus a later version of mail order, television shopping);

- Retail stores – In this model, the consumer comes to a place of business (a store) and the supplier's staff are in place, providing a physical environment in which consumers shop and buy. Significant costs are involved in retail stores, including the physical plant, inventory staff, advertising, and so on.
- Direct sales – In this model, the supplier visits the customer's residence. Direct sales effort by door-to-door salespeople and multilevel marketing (often used to sell cosmetics or household items) existed prior to EC, but have only limited relationship to its evolution.
- Mail order – In this model, the supplier and customer transact business without meeting. Mail order, for example, is based on printed catalogs from which shoppers choose their products and either mail, call, or fax in their orders. Mail order may also be costly, but it offers key advantages: it is "open" 24 hours per day, may reach a national or global market without the need for multiple store locations, and is highly flexible.

B2C EC may lower the cost of traditional retail operations. Internet business development is also moving towards new business models that fit the requirements of the consumer. For example, mass marketing is moving to a focus on targeted customer segments and terms such as Customer Relationship Management (CRM) are becoming more common. Other models are developing, such as auction sites, or service providers. This means that specialised forms of business are emerging that fit the business' market objectives by responding to the needs of targeted customers. "Today, most online B2C transactions are conducted using credit cards" (PWC, 1998); Potter, 2001).

The background on B2B and B2C above shows that payments are an essential element of both categories. This dissertation focuses on the payment process and the security around payments for Internet EC. The next section will highlight the payment systems for EC.

3.2.5 ELECTRONIC COMMERCE PAYMENT SYSTEMS

For EC to work, effective methods for paying for goods and services are necessary. This paper focuses on the risks and controls around Internet payments and the following section therefore provide background information for different payment systems. This will aid in the future analysis of the risks and controls around the payments. According to PWC research (1998), three payment methods are emerging.

1. Processes that use existing credit-/debit-card models – Card payment schemes provide a payment mechanism through the secure use of the existing credit- and debit-card payment infrastructure.
2. Electronic funds transfer using a cheque metaphor – A digital cheque is an electronic representation of a cheque; instead of being written on paper, it is digitally created, signed, and delivered. Like a paper cheque, a digital cheque is an instruction to the account holder's bank to transfer funds to a third party upon presentation of the cheque. It uses the existing interbank clearing process for cheque payments and settlements, operates in the same legal framework as its paper counterpart, and with the appropriate software, in principle may be used with current bank cheque accounts.
3. Electronic monetary alternatives – Electronic or digital cash is an electronic replacement for paper currency and coins. It provides the ability to transfer

value, in the form of digital tokens, between a buyer and a seller in exchange for goods or services, ideally without an intervening third-party validation and clearing of each transaction. Either cryptographic authentication or tamperproof hardware (such as a smart card) is required to prevent double spending or counterfeiting. Digital cash will be covered in more detail below.

According to Kabay (1998) "the buying public are leery of engaging in electronic commerce largely because they worry that their electronic transactions will be insecure. Observers in the growing field of e-commerce concur that lack of consumer confidence is the key stumbling block to continued growth of business on the World Wide Web." This aspect is also emphasised in the studies by the Singapore government (Singapore government, 1999), and Ecommerceabout (2001).

3.2.5.1 Online Payment Risks

Although the issues around risks and controls for EC payments will be discussed in the next few chapters in detail, some background information is presented below as an introduction. The problem of Internet security is in principle quite simple because an Internet connection potentially exposes a previously secure system to the world. The issue is not about having a Web site through which external users access a company system. The problem is simply being connected to the Internet at all. An Internet connection is a gateway to the external world, through which anyone with Internet access may attempt to break into an internal computer system. The issue to resolve is how to admit legitimate visitors and keep others out.

All security issues, and the attendant business risks, come together over the issue of online payment. Because of the inherent vulnerability of the Internet, e-business transactions require far more rigorous security to protect confidentiality of the transactions that occur, and of the transfer of high-value assets. According to Garceau (Garceau et al, 1998) "today the most common form of payment on the Internet is the credit card". Duquis (Duquis & Staglin, 2000) also shows the role of credit cards as the most common form of payment still in use. Payments through credit cards are of relatively minor concern in B2C Internet commerce because many security problems are solved by credit cards. Credit cards allow spontaneous transactions without the need for individual buyers and sellers to know and trust one another. For security, card users depend on an intermediary such as an issuing bank or credit card company that qualifies individual cardholders, extends them credit,

does credit checks and revokes cards for lack of payment, and constantly detects and manages fraud.

If network security is compromised and an improper transaction takes place, the established credit card infrastructure will handle the problem, guaranteeing, for example, that merchants will be paid and that, under certain laws, users are liable for only a limited amount of a fraudulent transaction. Therefore, the current Internet payment system does not introduce any more risk into the payment process than the model that is currently supported by the normal telephone system.

This does not apply to B2B transactions. Because they may involve large amounts of money and may contain highly sensitive corporate data, they need a better security platform than the ones provided with credit card systems. "In the B2B model that currently exists, there is no substitute for the credit card on a wide-scale basis" (Siebel & House, 1999). Today, each time a company seeks a new business partner, it must qualify the buyer or seller, check credit, negotiate terms, set up accounts payable and receivable, and incur the costs of order-taking, invoicing, payment, and collection. It may be an expensive process.

The above sections provide the background for the two most common EC categories. There is a close link between the EC categories and the payment systems in EC e.g., credit cards and B2C commerce. The security around payments is therefore also a critical aspect of EC. The risks around payments need to be identified and addressed through controls so that customers and business partners will be able to do business with an organisation with confidence.

3.2.5.2 Internet Payment Security

Payment security is critical to the success of e-commerce (Baltimore 1999; Hinton 2000; Entrust 1998; Symantec 2000; Ghosh 1997; & Hinton 2000). In examining the developments of payment security, the following are highlighted (PWC, 1998):

> Early EC transactions were conducted using standard e-mail or Web forms to send the buyer's credit card data to the seller without any special security. As security and privacy issues increasingly became important, the use of encryption and secure payment processes for online transactions evolved. The most popular process in use today uses SSL, developed by Netscape but

now a de facto standard (Ghosh, 1997) for encrypting data sent between a user's browser and the merchant's server. Although SSL initially was perceived as not sufficient for a robust commercial environment, secure transaction methods other than SSL are having difficulty gaining acceptance in the marketplace.

Today the most frequently used EC method (PWC, 1998) is still "a transaction carried out via an encrypted Web session by a buyer who trusts the merchant to provide goods and services as expected." As the level of Internet sales grows, concerns regarding fraud on the part of the buyer or the merchant increase. The two-party transaction with encryption (SSL) may become a three-party transaction, with the third party certifying the identity of the buyer and the seller through techniques that validate and authenticate both parties.

Processes to authenticate participants through the issuance of certificates are provided by protocols such as Secure Electronic Transactions (SET). (Third-party service providers that guarantee the validity of participants is another alternative.) Aspects such as SSL and SET will be covered in more detail in the following chapters, which address the solutions to the risks of EC payment systems.

3.2.5.3 Non-Credit Card Approaches

"Although most online B2C transactions still are conducted using credit cards in some way, payment technologies not based on the credit card model also are evolving for conducting online sales" (PWC, 1998). Other methods receiving attention include electronic cash such as CyberCoins and DigiCash (which may also be stored on an electronic wallet or on a smart card); stored-value (smart) cards such as Mondex and VisaCash; and micropayments.

This dissertation focuses on the risks and controls governing electronic commerce payments. Although the credit card is still the most common form of payment over the Internet, the non-credit card approaches are also being used. Therefore, any study of electronic payments should also include these non-credit card models, so that the background will be complete and these models should be included in the subsequent risk analysis and control identification process. The next section provides background on these non-credit card approaches to electronic payments.

3.2.5.3.1 Digital Money

It is now necessary to provide a short description of digital money and digital cash because the Internet seems to lack a standard form of digital money - some kind of fast, easy, and secure way to let consumers buy and sell electronically. Many merchants' practices, and many popular Internet-based payment systems are still based on credit cards. According to Siebel (Siebel & House, 1999) "a rash of high-profile security issues has caused many people to lose faith with credit card encryption as a truly secure line for electronic payment. Hence the emergence of digital cash alternatives".

3.2.5.3.2 Digital Cash

The alternative to arrangements that link payment to the buyer's existing credit or debit relationship with a bank is digital (or electronic) cash. The idea behind digital cash is that buyers possess tokens that may be exchanged for goods and services. In many cases, these tokens are used anonymously; that is, buyers use digital cash like ordinary cash, and there is no audit trail connecting the buyer to the purchase. This process accomplishes two goals. Firstly, the transaction is less expensive to execute because there is no need to authorise and then process a credit card transaction. Digital cash therefore opens the door for small purchases, such as an issue of an electronic newsletter. Secondly, digital cash approaches protect the privacy of the buyer, who may be reluctant to have an electronic record created of every purchase they make online.

The exchange of digital cash represents the exchange of electronic tokens (Berbera et al, 1997). In an electronic token system, tokens may be stored on a user's card or computer and may be exchanged directly between remote transacting parties. This exchange does not require a fixed network infrastructure and may be accomplished through an intermittent network connection or even a handheld device. According to Siebel (Siebel & House, 1999) "electronic cash replacements have had trouble gaining public mind share. In consummating online transactions, most people still depend, despite all of their protestations to the contrary, on their credit cards".

The conclusion that is drawn from this is that there is a perception that electronic money isn't "real" money. Electronic cash represents nothing tangible except an electronic number, first in a bank account, then as a set of electrons passing along a wire to a home computer, and then as an arrangement of magnetic domains on a hard disk. When a payment is made, signals are sent from the buyer's computer to another computer, and although the buyer's balance is debited, nothing concrete is handled.

Credit cards may then also be classified as not being real money, either. This may also be said of any currency bill that a Treasury Department issues. "All money is a conventional marker of value. It's just that plastic 'money' has been around for decades, and the electronic equivalent is still struggling for general recognition" (Siebel & House, 1999).

There are some advantages of electronic cash over credit cards. Firstly, it operates much like an ATM. A customer withdraws a certain amount and carries it away from the bank. Because a credit card involves a credit transaction, there are a lot of steps in the process, each contributing unavoidable processing fees. E-cash is carried on a computer instead of on a person and is transferred by wires. And because of the minimal processing fees (zero in some cases), even small payments may be made.

According to Siebel: "Each amount of e-cash carries an irrefutable signature from the bank that issued it - a highly secure digital signature. This makes it very difficult if not impossible to counterfeit. Even though each piece of e-cash also carries a unique serial number that only your computer could generate, the bank cannot know what this serial number is and thus can't trace any purchase or payment you make through e-cash back to its source." E-cash is therefore completely anonymous, just like paper money.

Another advantage with e-cash is that it is possible to prove beyond any doubt that a specific payment to a specific party came from a specific person, and only that person. For example, if someone was the source of an e-cash payment to a black marketer or extortionist, this could be absolutely determined with their cooperation and with data from their computer. So replacing paper and coins with e-cash will make life much more difficult for future criminals.

3.2.5.4 Other Non-credit Card Approaches

3.2.5.4.1 Electronic Wallets

A wallet is defined (whatis, 2000) as "a small software program and data that is used for online purchase transactions. Currently, CyberCash allows the consumer to get free wallet software that allows several methods of payment to be defined within the wallet (for example, several different credit cards)." This process works as follows for one of the wallet software products (whatis, 2000).

- "When you order something, the order is sent to the merchant. The merchant (actually, the merchant's server) sends back an invoice and asks the consumer to launch the Wallet in his computer (or to download it quickly if the consumer doesn't have it yet).
- When the consumer selects 'Pay', the software on the merchant server sends a message back to the consumer's PC that activates the "Wallet" software. The consumer selects one of the cards defined in the Wallet and clicks.
- The transaction includes real-time credit card authorization.
- CyberCash says "soon we will incorporate an electronic 'Cash' and 'Coin' system to use for transactions that are considered small for credit cards".

Electronic wallets are used by consumers to validate merchant servers, secure transaction information and payments, and store transaction data. Many EC software vendors have created their own wallets, which may be downloaded free from a merchant site that is using that particular company's server application and are stored on the user's PC. Although an electronic wallet is not necessary for existing EC transactions using SSL, it is a critical component of SET because the SET digital certificate is stored there. SSL and SET were mentioned briefly earlier on in this chapter, but will be discussed in more detail in the following chapters.

Wallet vendors include Netscape, Microsoft, CyberCash, IBM, Sun, and VeriFone.

3.2.5.4.2 Stored-Value (Smart) Cards

Stored value cards (cards that carry a certain amount of virtual cash stored directly on the chip and do not require online verification of that amount) help reduce transaction costs by allowing consumers to purchase low-price items without a credit card and without the merchant needing to verify each transaction. This approach allows users to gain the portability necessary to shop from any device equipped with a compatible smart card reader.

3.2.5.4.3 EC Payment Processors

Credit card transaction processors are critical to the B2C marketplace. A company may create an online storefront, fill it with products, and invite online customers, but the applications themselves cannot process credit cards or provide critical services such as fraud detection. "The key to effectiveness for transaction processors is the integration of their functionality with back-end applications" (PWC, 1998).

3.2.5.4.3.1 Payment Processing Software Vendors

Web merchants are able to ensure that a credit card number submitted to them is valid through a link to the credit card authorisation network. However, this process may be too costly for smaller EC sites. Furthermore, it only guarantees the card number is valid, without guaranteeing the person placing the order is the legitimate cardholder. "Without SET, Web sites have no means of verifying the identity of the person placing the order" (PWC, 1998).

EC sites use a processing service that provides software and has access to the host bank's payment networks to perform credit-card verification. Some representative transaction processing vendors are listed below. Most fraud detection systems currently deployed on the networks of financial institutions rely on a neural network or "fuzzy logic" approach to fraud, allowing the software to capture suspicious transactions.

CyberCash provides both software and transaction processing services; the software is free, and the transaction processing generates the fees (i.e., it collects its fees from the banks processing the credit cards). Because of the volume of bank transactions it handles, CyberCash charges merchants a relatively low per

transaction fee. Because all CyberCash transactions are handled over the Internet, merchants do not have to worry about leased lines or dial-up connections to banks, making this an affordable option for companies just getting started in EC on the Web.

CyberSource, another service provider, provides fraud detection using its own technology. It collects more than 30 pieces of data and performs more than 150 calculations, looking at factors such as spending trends, and where the credit card is being issued to produce a weighted score that allows a merchant to accept or reject an order.

Payment mechanisms and the security around payments form the basis of this dissertation. The above examples provide background on the different payment alternatives available. This understanding will be used in the following chapters and will assist IS auditors to understand the Internet payment environment, which in turn will enable them to perform a preliminary risk analysis on the environment. From this risk analysis it is further possible to identify the possible controls to mitigate the risks.

3.3 CONTROL MECHANISMS

Although these are discussed in more detail in Chapter 5, it is necessary to briefly mention examples of the control mechanisms or technologies in use today, to aid in obtaining a complete overview and understanding of e-commerce. This complete overview will then be used in the next chapters to identify the risks associated with EC payments as well as to identify the controls necessary to address the risks. The risks and controls will then be translated into an audit approach, which may be used by the IS auditor involved in the audit of EC payments over the Internet.

3.3.1 ENCRYPTION

It is possible to keep unwanted users outside a company's systems through a coding process known as encryption. If data is sent as unmodified 'clear text', it is harmfully available to anyone who cares to read it, whether it is the intended party or not. If someone is involved in an online transaction and it is sent in clear text, someone could potentially intercept a name, address, and credit card number. But not if it's in code and that's why encryption is used. But encryption, as logical as it sounds, is not without problems. Among them is the issue of government limitations.

The United States government defines what level of security is legal (Garfinkel & Spafford, 1997), and this level is controlled by something quite simple in principle, the size (in bits) of the security key used to encrypt. While it is always a difficult operation to decrypt any encrypted message, the smaller the key, the easier it is to break a code, which means that the 40-bit code is more vulnerable than the 56-bit code.

3.3.2 AUTHENTICATION

In any business transaction both parties need to offer a guarantee of their identities. Sometimes authentication is as simple as providing a password. In e-business, authentication is accomplished in a number of ways, including the use of encryption technologies that perform authentication as well as encryption (Kabay, 1998).

Authentication requires, among other things, a digital 'signature' (Garfinkel & Spafford, 1997). The process begins with a mathematical summary called the 'hash code', which acts as a compressed representation and unique 'fingerprint' of the message. The hash code is then encrypted with the sender's private key attached to the message. When the message is received, the hash code attached to the message is compared to another hash code calculated by the recipient. If the two match, then the recipient knows that the message has indeed come from the sender, that it has not been altered, and that its integrity has not been compromised.

Keys for digital signatures are filed in a public-key directory, made up of individual user 'certificates' that serve to verify identities, like a bank's physical signature cards. A trusted certification authority manages and distributes these certificates, in addition to electronic keys.

3.3.3 ACCESS CONTROL

Access control determines who gets access to a local or remote computer system or network, as well as what privileges are granted when he or she logs on. Access to information may be restricted at the document level by access-control lists, which itemise the resources that individual users are allowed to access. In addition, access control mechanisms may be distributed on the network. The mechanisms do not have to reside on the same host as the Web site. This means that administrators may physically operate the access-control services on a separate host, allowing multiple Web sites to make use of the same access control mechanisms.

Another mechanism being used is 'smart cards', which complement the existing log-on methods. With a reader attached to the client, absolutely secure client/server authorisation is made possible, guaranteeing that the card is trusted. Stealing the card will of course give the holder an additional opportunity to break in, but the combination of a simple PIN number and the card makes unauthorised access much more difficult.

To limit movements of data between companies and customers, companies adopt various security measures to create what is commonly known as a protective 'firewall'. A firewall (Siebel & House, 1999) "can be software, hardware, or a combination of the two. Its principle function is to serve as an application-level gateway, allowing safe external connections to internal applications." Software and application access rules must be defined, and must be unique to a given application. Used correctly (Siebel & House, 1999), "application gateways provide a high level of security and should make it almost impossible for untrusted external users to execute an internal application - such as, for example, a company's accounts receivable software."

The controls mentioned above, encryption, authentication and access control, are essential elements of e-commerce. The fears of users or customers need to be addressed, as they are a limitation to the success of a company's e-commerce ventures. The controls will be discussed in the next two chapters in more detail.

3.4 CONCLUSION

The above discussion on electronic commerce highlights the fact that electronic commerce is a very new technology which will be important to future business and therefore to the IS auditors. There are many aspects to the e-commerce technology that must be understood by the IS auditor. Especially in the areas of electronic payments there are many vulnerabilities that need to be addressed. Auditors must be aware of all the vulnerabilities as well as the controls available to address these risks. The following chapters will provide a deeper insight into the risks and controls available in EC payment systems.

CHAPTER 4

RISKS IN E-COMMERCE PAYMENT SECURITY

INDEX

4.1 INTRODUCTION

The steps that the IS Auditor follows during an audit of e-commerce (EC) payment security is, firstly, to gather information related to the area being audited. Secondly, it is to identify the risks prevalent in the environment being audited, and thirdly, to identify possible controls that may be implemented to mitigate the identified risks. The last step (for the purposes of this dissertation) is to develop an audit approach to serve as a framework for the area under review. Other steps in the audit approach includes audit testing and reporting on the results of the testing. All these steps are designed so that there is an inter-dependency between the steps. The output of each step will serve as the input of the following step. For example, the risk identification process can not take place effectively without the background information.

In Chapter 3 information was provided to serve as background to EC payment security. In that chapter it was shown that the nature of the EC environment results in specific risks. These risks and the controls implemented to minimise them, is the main focus of the IS audit. This chapter will provide more detail regarding security and the risks around EC payments. This risk identification process, described in section 4.4 below, serves a twofold purpose. Firstly, it is clear that the risk identification process is essential to developing the audit approach, because, without this risk identification process, the IS auditor cannot determine where the focus of a review should be. Secondly, the risk identification process also assists the auditor to obtain a better understanding of the environment being audited.

Once the risks described in this chapter have been identified, the next step will be to identify possible controls to mitigate the risks (control identification is addressed in Chapter 5). The risk and control identification will then provide the foundation that will enable the IS auditor to formulate the audit approach for the audit of EC payment security (the audit approach is addressed in Chapter 6).

This chapter will firstly provide examples of security issues in e-commerce payments. Thereafter the need for security will be stressed, and a definition of security and the implications of the Internet on security will be provided. The IS auditor will then be able to identify the risks (threats and concerns) prevalent in the EC payment security environment.

4.2 SECURITY AND E-COMMERCE (EC)

EC is widely viewed as threatening the privacy of an individual. Several surveys indicate considerable concern by users about their privacy online. This aspect was also highlighted in Chapters 1 and 3. Additional examples emphasising these concerns follow.

- "In March 1997, the Boston Consulting Group (BCG) surveyed 9,300 people about privacy concerns. BCG found 76% of respondents expressed concern about sites monitoring browsing on Net; 78% said privacy assurance would increase their willingness to disclose private information on Net. Without privacy assurance, BCG expect $6B of Web business compared with $12B if privacy were assured" (Kabay, 1998).
- The Lou Harris organisation surveyed 1,009 computer users in a United States national sample. "More than 50% of users are concerned about the release of their e-mail address by those responsible for the Web sites they visit. In general, observers feel that lack of consumer confidence is seriously limiting growth of e-commerce" (Kabay, 1998).
- In one large survey "70% of respondents were worried about safety of buying things online; 71% were more worried about Internet transfer of information than phone communications; and 42% said they refused to transmit registration information via the Internet. Several other observers report that lack of perceived privacy is a major block to the growth of e-commerce and that security is essential for e-commerce. Barriers to more effective e-commerce include poor security standards" (Kabay, 1998).

The 1998 FBI/Computer Security Institute survey found that "72% of security breaches resulted in financial loss. Although survey respondents reported net losses greater than $136 million, the monetary value of losses from information security breaches is difficult to estimate since companies are reluctant to admit compromise or loss due to concerns regarding client trust" (Zimits & Montano, 1998).

Table 1 below represents the average loss of different types of security attacks as presented in an FBI/CSI Computer Crime and Security survey (Zimits & Montano, 1998). This gives an indication of where the main focus of criminals resides when it comes to computer crime. This table shows that the main type of attack (where the

biggest losses are suffered) is through insiders such as employees. Although system penetration by an outsider is listed at the bottom of the table, it does not mean that this type of attack is not as serious. Companies may be reluctant to admit breach of their security by outsiders due to the possible impact of the negative publicity on their business.

Table 4.1 The Average Loss of Various Security Attacks

Type of Attack	Average Financial Loss ($)
Unauthorised Insider Access	$2,809,000
Theft of Proprietary Information	$1,677,000
Telecom Fraud	$539,000
Financial Fraud	$388,000
Sabotage	$86,000
System Penetration by Outsider	$86,000

Source: 1998/CSI/FBI Computer Crime & Security Survey

The following quote highlights the magnitude of the concern over Internet security. "A Net connection is a gateway to the external world, a doorway through which anyone with Internet access can attempt to break into your internal computer system" (Siebel & House, 1999).

Given this consensus (as highlighted above) that the Internet is not secure on its own (this will also be further highlighted below), this chapter focuses on the risks in this unsecure environment. This risk identification part is an important aspect for the IS auditor. This is also emphasised by Martin (2000). "E-commerce comes with its own set of challenges for auditors, and perhaps security is the most important of all." Auditors should be aware of security management issues and have a sound understanding of the various security risks and the tools available to be used in e-commerce sites to provide the necessary protection.

4.3 THE SECURITY IMPLICATIONS OF THE INTERNET AS AN OPEN NETWORK

This next section will provide background information that explains why the Internet is considered to be insecure. To understand the openness of the Internet is essential for the IS auditor so that this information will aid in the identification of the risks involved.

The Internet is considered a world-wide, global information infrastructure. Industry and governments aim to reduce overheads and shrink budgets but still need to continue to provide high levels of service to their customers and trading partners. In order to fulfill their promise "open networks must provide an efficient, highly scalable way to transmit quantities of information from point to point while doing so with a high degree of assurance" (Masse & Fernandes, 1997).

Open networks, such as the Internet, obey rules, which differ quite materially from the traditional, switched, point to point telecommunications infrastructure (Masse & Fernandes, 1997); (Rutgers, 1998). The telecommunications infrastructure is not extra-ordinarily secure and lends itself quite readily to both legal and illegal interception of traffic by such methods as wire tapping. Open networks like the Internet rely on their openness to achieve their ends: packets must be easily inspected by each node encountered on their route across the wired and networked globe so that they will be handed off in the probable direction of their intended destination (Rutgers, 1998); (Mehta, 1999). According to Oscar (1999) and the FDIC (1999) "The Internet is inherently insecure. By design, it is an open network, which facilitates the flow of information between computers". This openness is generally recognized as "providing a medium which is too insecure to permit digital commerce to flourish as it ought to do normally" (Masse & Fernandes, 1997).

According to Masse (Masse & Fernandes, 1997) "in order to flourish, commerce requires a communications medium, which is sufficiently secure, in relative terms, to assure both the integrity of the message and the authentication of its source and destination." This opinion is also shared by KPMG (1995).

In data communications however, the traditional authentication and verification tools no longer work. It is possible to verify that a message was received integrally in a point to point data communication by periodically transmitting data back to the sender for verification against the bits originally sent, but there is no way of knowing precisely who the reply is coming from (Vandenoever, 1995). As an example of data communications failure - every day clerks in businesses all over the world transmit faxes to the wrong destination by inadvertently keying in the wrong telephone number. No one knows this until the intended recipient denies receiving the message. In the case of the open network, communications may be diverted, copied, altered, replayed, rerouted, etc. The Internet is notoriously insecure. This aspect is

emphasised by McGhie & Maier (1998); Siegel (1997); Blunt (1997); Walder (1999); Hartman (2001); Kabay (1998); Baltimore (1999); Miller (2000); Masse & Fernandes (1997). The view of PWC (2000) on this aspect is that "the more open your network, the greater the chance that someone with malicious intent can break in and wreak havoc on the systems that run your business". This openness aspect will be elaborated upon below.

The Internet is the dominant and most important global example of an open network and there are a good number of examples in the retail sector of businesses doing well with Internet commerce at the present time. Many examples of such businesses were provided in Chapters 1 and 3.

Areas of concern over the use of open networks for commercial traffic relate to the health and financial sectors. There are formidable amounts of information recorded, stored and transmitted in the health care industry. The information is created and used by such diverse participants as medical professionals (doctors, nursing and para-medical staff), hospitals, clinics, insurance companies, governmental agencies, and patients. The same is true in the financial and accounting industry and the legal profession. Such information flows make up a very large component of business communications. These types of information require a higher standard of care. Medical, financial and legal information most frequently require to be reasonably protected from disclosure to the wrong parties. The present nature of Internet and other open networks fairly precludes their generalised use to carry such traffic. In fact, legal opinions have been given to the effect that "the Internet is not an appropriate medium for transmitting privileged information" (Masse & Fernandes, 1997). Zeus (2001) also shares this view. There are however ways to ensure that the confidentiality and integrity of messages is protected and these aspects will be highlighted in Chapter 5 - Controls.

Because the Internet has been designed to be 'open', the security aspect is also necessarily severely compromised. It is therefore necessary for the IS auditor to understand this inherent risk the weakness in security causes, because this knowledge will aid the IS auditor in the risk identification process as well as the subsequent control identification process (controls are addressed in Chapter 5). The risks will be identified in section 4.4 of this chapter.

4.4 INTERNET SECURITY - THREATS AND CONCERNS

4.4.1 THE NEED FOR INTERNET SECURITY

It is important to understand why we need security and the following paragraphs will highlight this importance. According to PWC (2000) "...there is no e-business without security". Feinmann (Feinmann et al, 1999) summarised the need for security as follows: "Not long ago only large corporations and companies needed to concern themselves with IT security issues. Their efforts to maintain ownership of information were the main focus of the field. This is no longer the case. Technology has become so prevalent that it affects almost every aspect of daily life. Computers are at the core of most businesses, ranging from trading systems used on the stock exchanges to the sports web page that delivers last night's scores. Computers are responsible for maintaining such things as bank accounts, medical records, and credit histories. Clearly, everyone who has a credit card or uses an Automated Teller Machine (ATM) must be concerned with the accuracy and privacy of their personal information; consequently, they must also be concerned with IT security."

According to Baltimore (1999) "we need information security not only to protect our assets, but also to enable us to take advantage of the new market opportunity. We need to have the same level of trust in the electronic world, as we have in the traditional world." The advantages of capturing a share of the e-commerce market have been highlighted in the previous chapters. For businesses that have a presence in this market on the Internet, the 'world' will be at their door and the consumers of the world are within their reach. The negative side is that "along with legitimate consumers, all kinds of malicious users may also be trying to gain access to on-line trader's information. Good security is therefore required" (Ghosh, 1999). The reason why web security requires special attention is mainly because the Internet is a two-way network, which allows organisations to publish information to users but also for criminals to access the equipment on which the information is stored. "The stunning growth of the Internet has spurred a new economy in which all aspects of the traditional payment infrastructure are being challenged." "... payment strategies are rapidly becoming a critical success component for companies buying and selling online" (Duques & Staglin, 2000). According to Ghosh (1997) "the number one rated concern for both businesses and consumers in establishing and participating in e-commerce is the potential loss of assets and privacy due to breaches in the security of commercial transactions and corporate computer systems."

There is a general opinion that the Internet environment is not secure and that the major concern for organisations doing business over the Internet is security of their systems and operations. This aspect is emphasised by McGhie & Maier (1998); Siegel (1997); Blunt (1997); Masse & Fernandes (1997); Walder (1999); Hartman (2001); Kabay (1998); Baltimore (1999); Miller (2000). In the same context "the lack of means for making secure electronic payments over the Internet is preventing the WWW from realising its full commercial potential" (Dixon, 1999).

"Today's business environment has different security requirements than traditional commerce" (PWCGlobal, 1999). According to PWC (1999) "the increasing use of the Internet – as an inexpensive virtual private network for electronic commerce… – has raised additional concerns about network security". "E-commerce generates some common IT risks, as well as some specific e-commerce risks" (Martin, 2000).

The following definitions are given to help understand security.

- "Security is about protecting valuable assets against loss, disclosure or damage" (Oliphant, 1999).
- "…security is about managing risk to mitigate some business information you are trying to protect from unauthorised parties, and it is also about decreasing the number of opportunities for the attacker to gain entry to your protected data". (Maung, 2001).
- Web security is defined as "a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organisations. Security protects you against unexpected behaviour" (Garfinkel & Spafford, 1997).
- Security is dynamic: every month there are new types of attacks, new viruses, and/or newly published security breaches. Internal configurations are also modified with new applications (even new versions of operating systems or upgrades), and new hardware installed (modems on a workstation creating a "backdoor") (Martin, 2000).

These definitions have one thing in common and that is to show that security is about the protection of assets through minimising the risks, whether those assets are information, computer equipment, or any other assets required in a business environment. In an environment such as the Internet, information is a very valuable

resource. Effective security creates an environment that facilitates electronic commerce and private communications. This means not only creating a climate that is safe from robbery and fraud, but also a place where business transactions may take place under commonly accepted legal standards. Although an unsecured Internet will not stop electronic commerce, "the expectations are that the well-publicized lack of security on the Internet discourages business and consumer transactions" (Zimits & Montano, 1998).

4.4.2 BACKGROUND TO INTERNET SECURITY RISKS

To understand the risks regarding the Internet, this section continues with background information that emphasises the points highlighted in the previous section and so provides a broader and more detailed definition of risk. Thereafter it elaborates on the threats regarding the Internet. The specific risks are then listed and discussed in the remainder of this section.

The new global culture of electronic information exchange and networking poses a greater threat than ever before of fraud, e-mail eavesdropping and data theft for both companies and individuals. Enterprises around the world "are deploying a new generation of distributed, business-critical applications - enabling delivery of new products and services on an unprecedented scale - over intranets (employees), extranets (trading partners), and the Internet (worldwide customers and prospects). These applications must be operated in a high-availability, high-security environment, in order to gain customer confidence and allow enterprises to exploit the advantages of the electronic marketplace - faster time-to-market, lower distribution costs, and greater access to global customers" (Verisign, 1999).

According to Walder (1999) "the most obvious problem with Internet security is that as soon as you connect your network to the Internet, you are effectively opening a data pipe to the outside world. This is necessary to provide outbound connections for all your network clients, but is just as likely to allow unwelcome intruders to wander around your confidential data if you are not careful."

Information security is a major issue facing electronic societies (Masse & Fernandes, 1997). As the information highway transcends borders, locked doors are no longer sufficient to protect one of the corporation's most valuable assets - information. Information security is needed not only to protect assets, but also to enable

organisations to take advantage of this new market opportunity. "One of the major inhibitors for e-commerce on the Internet is security and privacy issues" (Mehta, 1999). The original intention of the Internet was for research and sharing of information, mainly by providing easy accessibility. Thus, openness was a focus, not security.

The above paragraphs have shown that security is a problem in the Internet environment. These problems must be narrowed down to specific risks. This is necessary so that the IS auditor will be able to analyse and understand each risk and determine what possible controls may be implemented to minimise those risks. The controls will be discussed in Chapter 5.

4.4.3 A DEFINITION OF RISK

Risk is be defined as

- "...uncertain future events that could influence the achievement of the organisation's objectives, including strategic, financial, and compliance objectives" (PWC, 2001).
- A vulnerability "is the susceptibility of a situation to being compromised. A threat (risk) is an action or tool which can exploit and expose a vulnerability and therefore compromise the integrity of a given system" (Flanagan & Safdie, 1997).
- The *Oxford Dictionary* (seventh edition) defines risk as "chance or possibility of loss or bad consequence; danger".
- Risk analysis according to the Canadian Institute of Chartered Accountants (CICA, 1986) involves "considering the damage which can result from an event of an unfavourable nature" and " the likelihood of such an event occurring".
- Another definition, provided as part of the preparation for students taking the CISA exam (CISA, 2001), states the following: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets".

From these definitions and the background information given in the prior sections, it is clear that risk is concerned with the protection of the assets of an organisation. These assets also include information and they (assets) are usually used in the day-to-day operations of the organisation. The loss of such assets may endanger the

continuity of an organisation or may negatively impact on the profitability of an organisation.

4.4.4 THREATS IN ELECTRONIC COMMERCE PAYMENT SECURITY

The following threats have been identified as the threats of EC payments.

1. Unauthorised access (Netscape, 1999); (FDIC, 1999); (Oscar, 1999).
2. Data alteration/Integrity (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001); as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (Mackey & Gossels, 2000); (CISA, 2001); (FDIC, 1999); (Oscar, 1999); (James, 1999).
3. Breach of confidentiality including Spoofing (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001) as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (Mackey & Gossels, 2000); (CISA, 2001); (FDIC, 1999); (Oscar, 1999); (James, 1999).
4. Denial of Service/Availability. (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001) as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (CISA, 2001); (Oscar, 1999).
5. Repudiation (Netscape, 1999); (FDIC, 1999); (Oscar, 1999); (James, 1999).
6. Client side and web side vulnerabilities (Netscape, 1999); (Beck, 2001); (Maung, 2001).
7. Authentication (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (FDIC, 1999); (Oscar, 1999); (James, 1999).

The threats faced by business conducted through the Internet are not the same as those faced by storefront operations. Differences are in method, scale and geographical area. There may be hundreds of electronic attacks being mounted on key systems. Keeping up with the risks is challenging due to the Internet technology moving at a rapid pace. Problems are compounded since the technology is not mature. In addition, in the experience of the author, developments are typically made

without careful consideration to security. The risks listed above are explained in more detail in the paragraphs below. The IS auditor needs to understand the nature of each risk, which will enable the IS auditor to further identify controls available to address each risk. The control identification process will be addressed in detail in Chapter 5.

4.4.4.1 Unauthorised Access

For the purposes of this study, unauthorised access will be included with the other risks mentioned (e.g., integrity, confidentiality, denial of service, etc.) because the possible results of unauthorised access are data alteration, compromise of integrity, breach of confidentiality, denial of service and/or repudiation. In the next three sections (4.4.4.2 to 4.4.4) unauthorised access is an integral part of the discussion.

4.4.4.2 Data Alteration/Integrity

Integrity means "the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness" (GASSP, 1997). Data integrity issues are usually accidental or malicious (Mehta, 1999). However, data integrity issues are more likely to arise from system and communication errors. Another definition provided by PWCGlobal (1999) states that integrity concerns "... the prevention of unauthorised modification of information. Data integrity refers to the requirement that data in a file remains unchanged or that any data received matches exactly what was sent".

According to Dfat (2000) integrity means "ensuring that information in the message (including the identity of the sender and receiver) is not accidentally or deliberately modified." Ghosh (1997) is of the opinion that "violations in integrity of data sent over networks are often incidental and unintentional, but the potential to maliciously alter data in order to affect some outcome exists."

The risk of integrity therefore involves the maintenance of the completeness and accuracy of the data. In an Internet environment the possibility exists that data may be altered during transmission from the sender to the receiver. A message may be sent to one or more customers or organisations. There are also many communication points (e.g., routers, firewalls, etc.) between the sender and receiver where a

message may be altered. Controls are available to ensure that the integrity of data is maintained. The controls will be addressed in detail in Chapter 5.

4.4.4.3 Breach of Confidentiality Including Spoofing, Data Theft, and Fraud

Confidentiality means "the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner" (GASSP, 1997). Data travelling over the Internet go through numerous intermediary sites and are routed considerably before reaching the final destination. A fixed path is not established for all messages passed between the message originator and its recipient. Thus, potential exists for people with the inclination to read information not intended for them. It is like sending a post card through surface mail. Additionally, the following is also stated regarding the Internet Protocol (IP). "IP is inherently insecure and provides opportunity for ill-intentioned individuals to read other people's transmissions" (Mehta, 1999). "One of the biggest fears that consumers have in online commerce is sending their credit card numbers over the Internet. It is quite easy for an interested party to eavesdrop on other people's Internet conversations" (Ghosh, 1999).

According to Mehta (1999) "the risks related to theft and fraud are probably more severe from Internet based transactions than when using traditional ways, especially in terms of scale." According to a joint survey by the FBI and the Computer Security Institute (CSI) of Fortune 500 companies (Mehta, 1999), "42 percent reported unauthorised use of their information systems, and 32 percent reported losing about $100 million due to security breaches, though not necessarily from the Internet." It is also important to note that electronic theft may be done from anywhere in the world. It becomes easier for a person to commit crime when hidden behind a curtain of electronic equipment such as routers, switches and wires. In addition, many companies may not have adequate controls to prevent and/or detect potential security breaches.

An example of spoofing (Netscape, 1999) occurs when "a virtual vandal creates a fake site masquerading as yours to steal data from unsuspecting customers or just disrupt your business." Spoofing is therefore also a way in which confidentiality may be compromised or in which fraudulent activity may take place.

Confidentiality involves the assurance that data is not disclosed to unauthorised persons. In the definitions and examples mentioned above, as well as from the previous two chapters, it becomes clear that privacy concerns are a major issue for EC. There are many possible ways in which privacy may be jeopardised, and these concerns need to be addressed to put customers and trading partners at ease when they deal with an organisation. There are controls available to ensure that the confidentiality of data is maintained and the controls will be addressed in Chapter 5.

4.4.4.4 Denial of Service/Availability

What is meant by availability is "the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner" (GASSP, 1997).

Denial of Service (DoS) attacks are defined (Mehta, 1999) as "launching an assault that would bring down the service that is offered to customers. Such attacks may cause loss of revenue when a company's key transaction server is brought down and customers cannot place orders." Netscape (1999) also agrees with this definition. This could also result in negative publicity when a Web-site has been altered. Unfortunately, it is difficult to defend against such attacks as infrastructural weaknesses are exploited. Knowledge of such attacks and other hacking/cracking related knowledge bases are well organised and published within the Internet community. A DoS "is aimed solely at making services unavailable. The attacks are particularly difficult to defend against because they exploit infrastructural weaknesses or flows in widely used protocols such as the Internet Protocol (IP). Strategically pinpointed attacks can bring down entire systems critical to the nation or organisation" (Ghosh, 1999).

DoS and availability is a concern and a risk because the unavailability of the medium used to conduct an organisation's business (in this case the computers) will result in a loss of revenue and/or customers. This will in turn have an impact on the long and/or short term profitability and continuity of the organisation.

4.4.4.5 Repudiation

Another concern is repudiation, especially for businesses where customers or business partners may deny that they transacted any business, when in reality, they

did (Mehta, 1999). For example, a customer orders a CD, and then denies to the vendor that such a request was ever made. In the Internet world, business parties may not know each other by face or reputation, or may not have had a prior business relationship. It would be difficult to positively confirm that a particular client did indeed request the transaction in question. Proper controls are needed to ensure for integrity and non-repudiation.

According to Dfat (2000), repudiation is summarised as follows: "The sender denies sending the message and the recipient disclaim receipt of the message".

Repudiation means that unnecessary costs may be incurred to prove that the transacting parties were the 'real' parties involved and therefore accountability is created. There are many ways to minimise and control repudiation risks and these will be addressed in the chapter on controls, Chapter 5.

4.4.4.6 Client side and web side vulnerabilities

Typical focus on e-commerce security has been on the transportation of information (Mehta, 1999). Often overlooked is the security of clients' PCs and Web servers. The biggest risk to clients connecting to the Internet is from the applications that are downloaded. These applications are typically downloaded by a click through to a Web-site that executes them within the PC. Such code typically animates Web pages. More and more Web sites are 'pushing' information to clients to make the Web servers more efficient. However, if the code downloaded has bugs or is malicious, risks could range from wiping clean the hard-drive to extracting information from the PC – often without the knowledge of the client. Though 'fixes' are constantly applied to the software, holes and vulnerabilities continue to emerge.

One of the obvious risks to Web servers mentioned above (4.3.4) is the denial of service attacks. Another issue is related to confidentiality of information that may be stored on Web servers, or areas that are accessible by Web servers such as database servers. If proper controls are not in place, this information could be retrieved, manipulated or destroyed.

Most security weaknesses of Web servers come from configuration issues. Typically, when installing the system, whether it is a firewall or an operating system, by default, a number of network services and protocols are made available. The more services

available, the more routes a hacker or cracker will have to penetrate the internal private network.

It is possible to protect data during transmission but this data will also be stored on a computer/server of an organisation. If this information is not protected at the server level, the integrity and confidentiality of the data are endangered and all controls implemented to protect the data during transmission will be rendered worthless. The controls related to client and web side vulnerabilities will be addressed in Chapter 5.

4.4.4.7 Authentication

Authentication involves the concern that "both parties quoted in the message are the actual parties to the transaction" (Dfat, 2000); (Held, 1997). This aspect has been addressed in the repudiation risk above because of the close link between the issues involved. For the purposes of this study authentication will be addressed in conjunction with repudiation issues.

4.4.5 RISKS RELATED TO SPECIFIC INTERNET PAYMENT METHODS

The main payment systems being used for Electronic Commerce (i.e. credit cards and electronic cash) have been mentioned in Chapter 3. The security problems affecting these two areas of Internet commerce are summarised in the following sections (4.4.5.1 and 4.4.5.2).

4.4.5.1 Credit Card Transactions

Confidential information, such as credit cards and personal details, may be intercepted during transmission over the Internet, for example when submitting an order form on the Web. The following statements emphasise the importance of credit cards in EC. "Protecting credit card numbers used in online transactions is the most often cited example of the need for web security" (Garfinkel & Spafford, 1997). "Credit card fraud is already a significant factor inhibiting consumer confidence in e-commerce" (Bohm et al, 2000). Duques (Duques & Staglin, 2000) states that "credit card fraud on the Internet is 12 times higher than at brick-and-mortar stores. Ensuring that business, merchants, and consumers have security and authentication services are critical to the widespread deployment of e-commerce."

The controls related to transmitted information is to ensure that

- it is inaccessible to anyone but sender and receiver (privacy/confidentiality),
- it has not been changed during transmission (integrity),
- the receiver will be sure it came from the sender and the sender will be sure the receiver is genuine (authenticity),
- the sender cannot deny he or she sent it (non-repudiation).

Without special software, all Internet traffic travels 'in the clear' and so anyone who monitors traffic is able to read it. This form of 'attack' is relatively easy to perpetrate using freely available "packet sniffing" software since the Internet has traditionally been a very 'open' network. "No special physical access is required (it is also possible to eavesdrop using network diagnostic hardware if you have physical access to the network cabling). Passwords and credit cards may be distinguished from the rest of the traffic using simple pattern matching algorithms" (Kabay, 1998). According to Ghosh (1997) "one of the biggest fears that consumers have in online commerce is sending their credit card numbers over the Internet".

Protecting transactions is only one element of the secure transaction problem. Once confidential information has been received from a client it must be protected on the server (client and web side vulnerabilities). Currently, Web servers are among the softest targets for hackers, largely due to the immaturity of the technology. The paragraphs above show that credit card concerns are very important. As has been highlighted in the previous chapters, credit card concerns are a limiting factor for the growth of EC. The risks mentioned in 4.3 above also apply to credit cards as one of the payment systems used for Internet transactions.

4.4.5.2 Electronic Cash

According to Warigan (1999) "security is perhaps the most critical aspect of electronic cash. It is the focus around which a successful electronic cash mechanism is structured and functions. The risks related specifically to electronic cash are summarised in the following few points.

- Electronic cash is loaded into a physical object, such as a smart card on a personal card computer. The data is secured by cryptographic methods. These

physical objects may be the subject of an attack (This is considered to be client and web side vulnerabilities).

- Electronic cash may be lost if the device e.g. computer that it is stored on crashes or if it is not protected by the owner or user (This will be considered under the client and web side vulnerabilities issues).
- The initiating system may be compromised resulting in the value of the cash to drop (This will be considered under the client and web side vulnerabilities issues).
- Software based electronic cash are susceptible to theft through hackers (This will be considered under the client and web side vulnerabilities issues).
- Privacy may be compromised by a lack of controls over electronic cash (This will be addressed under Confidentiality/ privacy issues).
- Electronic cash is protected through cryptographic solutions. All encryption or cryptographic mechanisms are breakable (Garfinkel & Spafford, 1997); (Warigan, 1999); (Ghosh, 1997).

Although electronic cash differs from credit cards in the sense that it is supposed to provide more anonymity, the main risks related to the use of this medium for electronic payments still revolves around the risks mentioned in section 4.4.3 above. The main security objective is to deter all or most people from attempting to compromise a secure mechanism and to make the cost of breaking such a mechanism higher than the benefit of doing so.

4.4.6 MANAGING THE RISK

The Internet's weakness (as an open network) is also its fundamental strength. The strength is that its openness makes it the ideal platform for global commerce and communications. The Internet offers the promise of inexpensive mass communication and provides economies of scale for low-cost distribution. This aspect has been highlighted in Chapters 1 and 3 of this study. However, the weakness of the Internet as highlighted above is that since it is open, communications are inherently difficult to secure. What is missing is the mechanism to guarantee the integrity and confidentiality of information and to provide protection against denial of service attacks, and to minimise exposures created by client and web side vulnerabilities. There are various controls available to address the risks highlighted in this chapter. These controls will be discussed in Chapter 5.

In the face of massive enthusiasm for the Internet, it must be stressed that 'all security is relative'. Any practical answer to the problems has to be a compromise between vulnerability and risk (e.g. there are some vulnerabilities which only a handful of people are currently skilled enough to exploit, which implies that the likelihood of the vulnerability materializing as an actual threat is relatively minor). The assessment of each threat must be weighed against what is at stake, the exposure faced by proceeding with the knowledge that some attacks are possible.

To manage business risk, the prudent business must therefore deal with risk by

- firstly, identifying the risks it runs (as described in section 4.4.4 above);
- secondly, avoiding those risks which may reasonably be avoided. This is done through the implementation of controls to minimise the risks- as described in Chapter 5);
- thirdly, shielding itself from the risks it cannot avoid principally by declining liability through contract or benefiting from so-called legislative safe-harbour provisions,
- and finally, accepting those risks which it can neither avoid nor deter by insuring, hedging, financing or otherwise providing for the impact of the risk on its business.

4.5 CONCLUSION

The approach to an IS audit of EC payment security involves a number of steps. It starts with the understanding of the environment and follows with the identification of risks. This chapter identified the unique risks in the EC payment environment. These risks stem from the fact that the Internet has been designed to be 'open', which increases the likelihood of manipulation. The need for security and control in this environment has also been highlighted. It has been established that the IS auditor needs to be aware of the inherent risks in an EC payment security environment so that it will enable him/her to identify such risks when an area involved in EC payments is being evaluated/reviewed. This chapter identified seven threats/risks in the EC payment security environment.

The IS auditor plays an important role in the risk management process through the risk identification process, and armed with knowledge of the risks, the IS auditor is able to perform the next step in the audit approach, which is to identify the controls

required to minimise or manage the risks identified. The ultimate objective of the audit is to form an opinion regarding the control environment.

CHAPTER 5

CONTROL IDENTIFICATION FOR E-COMMERCE PAYMENT SECURITY

INDEX

5.1 INTRODUCTION

The approach of the IS Auditor to an audit, including an audit of e-commerce (EC) payment security is (CISA, 2001); (Perry, 1983); (SAICA, 1998) firstly to gather information related to the area being audited. Secondly, to identify the risks prevalent in the environment being audited, and thirdly, to identify possible controls that, if implemented, will mitigate the identified risks. The last step is to develop an audit approach to serve as a framework for the area under review. These steps are designed so that there is an inter-dependency between the steps. The output of each step will serve as the input of the following step. For example, the controls identification process cannot take place effectively without the risks being identified.

In chapter 3, information was provided to serve as background to EC payment security. In that chapter an introduction was also given to the risks in EC payment systems. Chapter 4 provided more detail regarding security and the risks around EC payments. This chapter will address the possible controls that, if implemented, will mitigate the risks. This is an essential step for the IS auditor, because, without this control identification process, the IS auditor cannot develop an audit program.

The objectives of this study is to provide background information for the IS auditor when auditing EC payment security and ultimately to develop an audit approach for this area. The controls identification process therefore serves a twofold purpose. Firstly, from the audit approach highlighted above, it is clear that the control identification process is essential before the approach can be developed. Secondly, the control identification process also assists the auditor in obtaining a better understanding of the technology available to address the risks prevalent in the EC payment security environment.

Once the possible controls have been identified as described in this chapter, the next step will be to combine the risk and control identification processes to provide the foundation that will enable the IS auditor to formulate the audit approach for the audit of EC payment security.

This Chapter is structured as follows:

1 Firstly provide an understanding of control and the role of controls in an organisation;

2 secondly, controls will be identified for each of the risk areas identified in chapter 4; and

3 thirdly, the technology available to provide the controls will be explained in more detail.

With the knowledge obtained in this chapter and the previous chapter, the IS auditor is able to identify the risks, identify possible controls to mitigate the risks, and develop an audit approach.

5.2 CONTROLS DEFINITION

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. According to ISACA (1999): "Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide. Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources." "Internal control system provides the discipline, consistency, and guidance to carry out organisation's mission and objectives" (Vallabhaneni, 1991).

Internal control (BC, 2001); (CICA, 1986); (Ams, 2001); (Vallabhaneni, 1991); (ISACA, 1999) comprises the plans, policies, practices, organisational structures, and procedures of an organisation and all the coordinate systems established by the management of the enterprise to assist in achieving management's objectives in the following categories:

- Safeguard its assets and records (Vallabhaneni, 1991); (Ams, 2001); (CICA, 1986); (Cooper, 1982),

- Verify the accuracy and reliability of its accounting data. (Ams, 2001); (BC, 2001), (CICA, 1986); (Cooper, 1982),
- Provide relevant (e.g. strategic, operational, tactical) information to management. (Ams, 2001),
- Promote operational efficiency and system economy and effectiveness. (Ams, 2001); (BC, 2001), (CICA, 1986),
- Encourage adherence to prescribed managerial policies, procedures, and standards. (Ams, 2001), and
- Comply with laws and regulations. (Ams, 2001); (BC, 2001).

Internal controls should also help recover from disasters of any kind (Vallabhaneni, 1991). According to Pomeranz (1992) "Internal control is management's procedure for addressing risk". Information systems control form part of the entity's internal control system. An entity's internal control system is composed of a number of individual controls. A control is described as "a procedure or a set of procedures that, individually or in combination with other controls, can assist in achieving the internal control objectives of the entity" (CICA, 1986).

Internal controls are either detective, corrective, or preventive by nature (Vallabhaneni, 1991); (Ams, 2001). Detective controls are designed to detect errors or irregularities that may have occurred. Corrective controls are designed to correct errors or irregularities that have been detected. Preventive controls are designed to keep errors or irregularities from occurring in the first place.

According to ISACA (1999):

> "Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same "leap frog" manner as the underlying computing and networking technologies are evolving. Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfill their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise

reasonable and prudent judgments in evaluating control practices found in typical business or governmental organisations."

According to the AARF (2000): "Although an IT security infrastructure and systems controls can help to manage risks, there is a degree of uncertainty which cannot be eliminated. For example, the use of evolving technology, and the risk of determined hackers overriding security means that some residual risk will remain despite controls put in place by the entity. Management decides on the level of acceptable risk to balance costs and benefits in the control system relating to e-com."

"Security isn't a technology problem, but a business problem" (PWC, 2000). Even with the best controls and mitigation strategies, there is still risk. Internet transactions can be made relatively secure but security to prevent unauthorised access is highly complex and technical, and residual risks mean that the risk of unauthorised access cannot be completely eliminated. Residual risk relates to that aspect of risk which remains after security controls have been implemented, and which arise in a dynamic electronic environment (AARF, 2000); (Lindner, 2001). For example, controls in place may become less effective as new technologies are introduced.

A total information security solution includes policy and procedure, access control, user authentication, encryption, and content security. The security of transactions over the Internet may be established by the implementation of various security measures or controls to address different risks. For example, security measures include encryption, digital signature or digital certificates (or public key encryption which collectively supports a digital certificate-based encryption system), firewalls, secure socket layers, etc. All these control aspects will be described in more detail in this chapter.

By focusing a security solution on an individual component, such as access control or an encryption method, there is a risk of leaving holes in the security shield that are available to be exploited by a hacker.

Approaching security as a concept and not as individual components is therefore the best way to develop and implement secured network environments. As shown in the above descriptions, the IS auditor needs to be aware of the evolving technologies due to the fact that with the changes required by the new technology, new risks are introduced and new controls are therefore required. The technologies highlighted in

this chapter will enable the IS auditor to understand the technology and identify possible controls in EC payment security audit environments.

5.3 ELECTRONIC COMMERCE CONTROLS BY RISK AREA

According to Mehta (1999) "the threats faced by business conducted through the Internet are not the same as those faced by storefront operations. Differences are in method, scale and geographical area." Keeping up with the risks in the Internet environment is challenging due to the Internet technology moving at a rapid pace. The technology has also not been used for extended periods of time and is therefore considered "not mature". "In addition, developments are typically made without careful consideration to security" (Mehta, 1999). In Chapter 4 on Risk, the following threats were identified:

- Breach of confidentiality
- Data alteration/integrity
- Unauthorised access
- Non-repudiation
- Denial of service
- Authentication
- Client and web-side vulnerabilities

The controls to minimise these threats will be covered in the remainder of Section 5.3 and also in Section 5.4. It is important for IS auditors to understand the controls available so that the IS auditors will be able to identify the controls applicable in each environment where they are involved in the audit of security of EC payments. Section 5.4 below highlights the controls available to address the risk.

5.3.1 INTERNET SECURITY ISSUES - PRIVACY AND CONFIDENTIALITY

Confidentiality is a security property that ensures that data is disclosed only to those authorized to use it, and that it is not disclosed to unauthorised parties (Techguide, 2000); (Dekker, 1997); (E-witness, 2001). This also means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, card expiration dates, and so on (Asokan et al, 1997); (VISA, 1997). This information provides the key elements needed to create

counterfeit cards and/or fraudulent transactions. The reason behind ensuring the confidentiality of information on the network is to deny information to anyone who is not specifically authorized to see it or use it and to ensure that information is not intercepted during transmission (Techguide, 2000); (Verisign, 1999).

Encryption is a frequently used mechanism for guaranteeing confidentiality (Techguide, 2000); (Rapp, 2001); (VISA, 1997); (Netscape, 2001); (E-witness, 2001); (Mackey & Gossels, 2000), since only those recipients who have access to the decrypting key are able to decode the messages. Encryption will be discussed in Section 5.4.1 below in more detail as one of the tools for controlling Internet payments.

5.3.2 INTEGRITY

Integrity refers to the completeness and reliability of the message as it passes through the network. The key is to make sure that the data passes from the source to the destination without alteration and to prove that information has not been manipulated (Techguide, 2000); (VISA, 1997); (Verisign, 1999); (Dekker, 1997); (E-witness, 2001); (IEC, 2000).
Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions (VISA, 1997). If any component is altered in transit, the transaction will not be processed accurately. To eliminate this potential source of fraud and/or error, a means must be provided to ensure that the contents of each order and payment message received matches the contents of the message sent.

The integrity of data in storage and in transit is assured through encryption and the use of digital certificates/signatures (Norton, 2000); (VISA, 1997); (E-witness, 2001); (Mackey & Gossels, 2000). Encryption, digital certificates, and digital signatures will be discussed in more detail in Section 5.4 below.

5.3.3 ACCESS CONTROL AND AUTHORISATION

Authorisation relates to the aspect of accepting or rejecting a particular requester to have access to some service or data in any given system (Techguide, 2000); (Kabay, 1998); (Dekker, 1997). In this context a requester could be a user, program or process; a service could be a program, a device such as a printer or a file system;

and data could be a text file, an image, a collection of files, or any combination of the above. For example, authorisation takes place every time a merchant queries VISA or MasterCard service to see if a customer is authorised to spend a certain amount of money at their establishment.

The risks involved in allowing access to individuals to system services or information must be considered. For example, in the case of advertising the Web page of an organization, allowing access means that limited damage could occur. The objective of such a page is to spread the word about the organization, and therefore access control is not an issue. On the other hand, access control is a major issue if someone requests access to the file, which contains the passwords of all of the users of the system. It is therefore necessary to define a set of access rights, privileges, and authorizations, and assign these to appropriate people within the domain of the system under analysis.

Authentication and authorization go hand in hand (E-witness, 2001) (Dekker, 1997). Users must be authenticated before carrying out the activity they are authorized to perform. According to Jones (2001), "authorisation is the final stage of access control." Therefore, when considering the controls for authorisation, the controls for authentication as discussed in 5.3.6 below also needs to be taken into account.

"A payment system with integrity allows no money to be taken from a user without explicit authorization by that user" (Asokan et al, 1997). Authorisation constitutes the most important relationship in a payment system.

In the mainframe environment, authorisation depends on the operating system and the level of security that system administrators have imposed (Kabay, 1998). Identification and authentication (I&A) begin when a session is initiated. A session is "an activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff)" (Kabay, 1998). Web interactions require I&A only when the user and the Web owner agree to establish a secure session. Typically, secure Web transactions do require some form of logon and logoff even if these steps are not explicitly labeled as such.

Access Controls are those policies, procedures, and tools that control access to resources (Norton, 2000). Logical access controls typically come into play in the form of system user profiles for access to network resources.

In essence, access control is implemented as a database of users and their privileges. At the infrastructure level, the Kerberos standard is commonly employed (PWC, 2001). Kerberos is a trusted authentication software system that through the use of shared secrets or keys, establishes a trusted end-to-end path or connection for use by two parties or processes (Deloitte & Touche, 1997); (Mackey & Gossels, 2000). Many application software suppliers also offer access mechanisms. In addition, the digital certificate is available to be used as the basis of access control. Firewalls are access control tools designed to provide access control protection. All these tools used in access controls (i.e., digital certificates, firewalls, etc.) are discussed in more detail in Section 5.4 below.

In summary, identification, authentication and authorization are normal components of any business transaction and must be guaranteed by the communications systems and software used between supplier and customer.

5.3.4 NON-REPUDIATION

This security concept protects against the sender or receiver denying that they sent or received certain communications and therefore ensuring that transactions, once committed to, are legally valid, irrevocable (Techguide, 2000); (Verisign, 1999); (Kabay, 1998); (Dekker, 1997); (E-witness, 2001) and cannot be disowned (Baltimore, 1999).

One definite way to ensure non-repudiation is established through the following key aspects (Martin1, 2000):

- Participating parties must authenticate each other.
- The integrity of the messages exchanged between the two parties must be controlled (e.g., encryption).
- Give a means whereby parties can electronically sign the contract (i.e., digital signature). This will ensure integrity and the signature will support non-repudiation.
- Keep the transaction confidential (privacy, access control).

As stated in Chapter 4, there is a very close relationship between repudiation and authentication and the controls used for authentication will also be used to establish

non-repudiation. According to Kabay: "Authentication leads to a related concept, that of non-repudiation. Non-repudiation depends on asserting that authenticity has not been violated when identifying the source of that transaction or message." The controls used for authentication are mentioned in Section 5.3.6 below and this section on non-repudiation needs to be reviewed/ interpreted in conjunction with Section 5.3.6. Control technology used to address non-repudiation include encryption, digital signatures and digital certificates (Martin1, 2000); (Mehta, 1999), and these aspects/technologies will be discussed in Section 5.4 below.

5.3.5 AVAILABILITY – DENIAL OF SERVICE (DOS)

It is possible for information to be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need (Dekker, 1997). Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable (Asokan et al, 1997); (Verisign, 1999). All parties require the ability to make or receive payments whenever necessary. According to Asokan (Asokan et al, 1997), "payment transactions must be atomic: they occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash."

In a DoS attack, a hacker gains access to several computers connected to the Internet and installs code on those systems. At the hacker's signal, the systems start sending data to targeted Web sites. The sudden burst of network traffic overloads the Web servers and the networks they are connected to, slowing performance and eventually crashing the site (PWC, 2000); (Scit, 1998).

When a DoS attack comes from several sources it is known as a "distributed denial of service" attack (or DDoS Attack) (Gregg, 2000); (Kessler, 2000). This is a method available to hackers to explore and exploit weaknesses in a company's Internet site. The method involves bombarding the web site with packets of information similar in nature to requests that would be sent by legitimate users. These attacks are usually performed via a series of compromised staging sites. This disguises the origin of the attack and preserves the anonymity of the hacker (Gregg, 2000); (Todd, 2000). The web site under attack may react in one of several ways. It will either shut down under the strain; continue to operate normally but legitimate users won't be able to access the site; or (worst case scenario) the defense mechanisms of the site break down

allowing the hackers complete access to the site and potentially the corporate networks behind it. "In most cases, disruption is highly likely" (Gregg, 2000).

DoS attacks may result in significant loss of time and money for many organisations (Fuller, 2000). Organisations should consider the extent to which they could afford any service outage and take steps to mitigate unacceptable risks. These steps/controls that are available to be implemented involve many of the other tools mentioned in Section 5.4 of this chapter. The following control options should be taken into account. (Note that for each option mentioned below, the tools that address the weakness are also identified. These tools are described in Section 5.4 of this chapter.)

- Establish and maintain regular backup schedules and policies, particularly for important configuration information (Fuller, 2000). Addresses server vulnerabilities.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts (Fuller, 2000); (Levy, 2000). Server vulnerabilities and access control.
- Implement properly designed firewalls. These track traffic in and out of the site, logging and inspect every packet of information to ensure its legitimacy (Fuller, 2000); (Gregg, 2000); (Mackey & Gossels, 2000); (Todd, 2000); (Kessler, 2000); (PCIS, 2000); (Cknow, 2000); (CERT, 1999). Firewalls.
- Keep all software up-to-date: Implementing all security fixes and patches as they are released will go a long way to reducing vulnerability to these attacks (Fuller, 2000); (Gregg, 2000); (Kessler, 2000); (PCIS, 2000); (Cknow, 2000); (CERT, 1999). As available, install patches to guard against TCP SYN flooding. Firewalls.
- Disable any unused or unneeded network services (Fuller, 2000); (Todd, 2000); (PCIS, 2000); (CERT, 1999). Firewalls and server vulnerabilities.
- Enable quota systems on operating system if available: limit users and programs to a specified amount of resources only (Fuller, 2000); (Levy, 2000). Server vulnerabilities.
- If the operating system supports partitions or volumes, partition the file system so as to separate critical functions from other activities (Fuller, 2000). Server vulnerabilities.
- Establish system performance baselines and observe daily activity for aberrations (Fuller, 2000). Server vulnerabilities.

- Routinely examine the physical security environment with respect to current needs (Fuller, 2000); (Unixtools, 2001). Server vulnerabilities and physical security.
- Use tools (e.g., Tripwire) to detect changes in configuration information or other files (Fuller, 2000); (Mackey & Gossels, 2000); (PCIS, 2000). Server vulnerabilities.
- Invest in fault-tolerant network configurations. (Fuller, 2000). IDS.
- Switch on audit logs for all key servers: when efficiently and effectively configured and monitored, these logs will provide adequate information to identify and investigate any problems (Gregg, 2000); (Kessler, 2000); (CERT, 1999); (Unixtools, 2001). IDS.
- Install intrusion detection software. If properly configured, this software will quickly identify known patterns of attack and immediately shut out only the attacker, while sounding the appropriate alarms (Gregg, 2000); (Mackey & Gossels, 2000); (Levy, 2000); (PCIS, 2000). IDS
- Hire the right people: make sure your technical personnel completely understand the issues, the technologies and the solutions (Gregg, 2000); (PCIS, 2000); (Ghostship, 2001).
- Test defenses regularly. The rapid rate of change in both the technology area and the hacking community means defenses must be tested on a regular basis (Gregg, 2000); (Mackey & Gossels, 2000); (Kessler, 2000); (PCIS, 2000); (Unixtools, 2001). IDS.
- Design the network to isolate attacks. If the worst happens and the hacker gets inside, appropriate network configuration, firewalls and other tools will ensure any damage the hacker could cause is isolated to a small area (Gregg, 2000). IDS and Firewalls.
- Have an incident response plan. Identifying, reacting to and resolving the problem immediately is the real business challenge. Most organizations implement the right preventative measures, but do not prepare and train for the worst. Identify who should respond and test the plan; establish procedures for determining the seriousness of the breach (Gregg, 2000); (PWC, 2000); (PCIS, 2000). IDS.
- Focus on preventative measures. Swift, large volume, automated attacks require sophisticated, automated defense mechanisms. Identifying a problem an hour later and then trying to trace and resolve it is not an option (Gregg, 2000); (Todd, 2000).

- Gather evidence. Understanding how to identify, gather and manage legal evidence to ensure the appropriate legal action can be taken against a hacker should be a key element of defense system design (Gregg, 2000).
- Educate the users. Constant awareness and updating of knowledge is the best defense to any attack (Gregg, 2000); (Pethia et al, 1991). Server vulnerabilities.
- Use network or file scanning tools to detect DdoS attacks and keep these up to date with new developments and types of attacks (Levy, 2000).

According to Gregg (2000), "even if these activities are all implemented correctly, an organisation may still not be able to guarantee 100% security - at least not as long as human error is a factor. That's the nature of doing e-business. What can be guaranteed is that the hacker will quickly tire of attempting to break down a company's defenses and move onto the next poorly protected site."

5.3.6 AUTHENTICATION

A primary tool in securing any computer system is the ability to recognize and verify the identity of users (individual, group, system, or application) (Techguide, 2000); (Verisign, 1999); (Kabay, 1998); (PWC, 2000); (Jones, 2001). This security feature is known as authentication. After being authenticated, the object is granted access to the services required, and its activities may be monitored (PWC, 2001). Authentication and authorisation together are the foundation of any security plan, and is often a key part of other security solutions (PWC, 2001). The authentication technology used to protect a particular resource should be determined by the resource's importance to the business. Authorisation was discussed in 3.3 above.

There are three generally accepted techniques for authenticating users to host servers (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998). These three factors are also sometimes referred to as multifactor authentication (PWC, 2001), and are detailed below.

1. *Authentication by something the user knows*. This is the password/username concept. Traditionally, special names and secret passwords have been used to authenticate users, but the password is only as good as the users' ability to keep it secret and protect it from being abused by unauthorized users (PWC, 2000); (Kabay,

1998); (Norton, 2000); (PWC, 2001); (Techguide, 2000); (Mehta, 1999); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998).

One of the methods for hackers and crackers to break into systems is by breaking into legitimate user accounts via cracking (or guessing) passwords. There are tools freely and publicly available to crack passwords for all sorts of systems. These tools are easily able to crack passwords due to the type of passwords selected by system users. Due to human nature, people tend to select passwords easy for them to retain such as children and pets' names, and other common English words (E-witness, 2001). Thus, using passwords for user authentication and authorisation is inherently weak (Mehta, 1999). Even encryption requires the use of codes and passwords (see encryption Section 5.4.1). Passwords are often the only wall between a hacker and privileged, proprietary and networked information.

2. *Authentication by something the user has.* In this technique, the user is given some kind of token, such as a magnetic stripe card (smartcard), or key (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998).

3. *Authentication by physical characteristics.* (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000), (VISA, 1997); (Martin1, 2000); (Mehta, 1999); (Dekker, 1997); (ZDnet, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998). Here, the mechanism is to recognise some measure of the individual, which cannot be duplicated. Biometric techniques such as fingerprint ID, palm print ID, retinal scan, manual and digital signature, or voice recognition are used to validate the identity of the potential user.

"Authentication is also necessary when two computers communicate with each other" (Mehta, 1999). For example, if another computer asks a host computer to have a disk mounted which contains all of an organisation's personnel data, it must be determined that the requesting computer has a legitimate reason to access that information, and that it is not some external network hacker trying to steal information from the organisation.

All of these categories of authentication are used on the Internet (Kabay, 1998).

Authentication is made possible by using shared-key or public-key cryptography, digital certificates, encryption and secure protocols (Asokan et al, 1997); (Feindt & Culpin, 1998). These methods will be discussed in Section 5.4 below.

The six areas mentioned in Section 5.3 above are all important in an EC payment security environment. The controls present in each of these areas will have an impact on the overall conclusion on the control environment. The detailed controls available for each of these six sections are through the various technologies mentioned in Section 5.4 below. The IS auditor must understand the controls required for each of these six areas in Section 5.3 above so that it will enable the IS auditor to develop an audit approach for EC payment security.

5.4 TECHNOLOGIES USED FOR CONTROL PURPOSES

To secure information and EC payment details on the Internet, many different technologies are being used in various combinations.

Integrated security architecture includes new mechanisms such as firewalls, VPNs, IDS, PKI, Digital certificates and secure protocols (these technologies will be described in Section 5.4 below). To secure the connected enterprise, the collection of techniques must be managed as a whole to ensure that enterprise assets are appropriately guarded i.e., no one solution alone is enough to secure the payments. The IS auditor needs to be aware of the different technologies being used (i.e., the IS auditor needs to have an understanding of technologies and what control each technology provides). This stems from the general requirement that the auditor needs to have "adequate technical training and proficiency as an auditor. (For example as prescribed by the AICPA General Standard ET201 (AICPA, 1997). Armed with this information, the IS auditor considers the relevance of the control in the area being reviewed and evaluate whether the effectiveness and efficiency of each control should be tested. The technology areas described in Sections 5.4.1 to 5.4.7 below should be considered while keeping this aspect in mind.

5.4.1 ENCRYPTION AND SECURE PROTOCOLS

5.4.1.1 Encryption

While information travels between the server and the browser, it may be stored on intermediate devices and may be intercepted and even modified by third parties (Dallas, 1998). Without additional effort, this structure provides neither privacy (confidentiality), nor integrity, nor authentication (Dekker, 1997); (CSE, 2001);

(Dallas, 1998). Encryption is the foundation for safe Internet commerce (Zimits & Montano, 1998); (Feindt & Culpin, 1998); (Hartman, 2001). It covers not just the coding or scrambling of messages but authentication, message integrity, non-repudiation, confidentiality of data, digital signatures and other security related issues (Asokan et al, 1997); (Feindt & Culpin, 1998); (Certicom, 1997).

Without encryption, messages containing sensitive private information or financial details, such as credit card numbers, may be read at numerous points as the messages pass through the net. Cryptographic techniques are essential tools in building secure payment systems over open networks that have little or no physical security. Using no cryptography at all means relying on out-band security (Asokan et al, 1997) e.g., goods ordered electronically are not delivered until a fax arrives from the payer confirming the order.

Encryption is a very old technique (Techguide, 2000); (James, 1999) used to protect sensitive information as it is transmitted from one location to another (Martin1, 2000). It is simply the scrambling of the transmitted text using a set of rules (called algorithms, which means mathematical manipulations) to produce unintelligible (encrypted) data (Techguide, 2000); (Norton, 2000); (Landrum, 2001); (Baltimore, 1999); (James, 1999); (Feindt & Culpin, 1998); (Rapp, 2001); (Dekker, 1997); (Widman, 1999); (Terena, 2001); (Jones, 2001); (Scit, 1998). This ensures confidentiality. The recipient may then use the same set of rules in reverse to unscramble the coded text and read the intended message. The key used must be kept secret between the two parties (Baltimore, 1999).

Powerful encryption exists with which to insure the confidentiality, integrity, authenticity, and non-repudiation of data (Cobb, 1999) (Dekker, 1997); (ZDnet, 1997); (Deloitte & Touche, 1997); (McDow, 2001). There are two primary encryption methods in use today (Cobb, 1999); (Martin1, 2000); (VISA, 1997); (Widman, 1999); (ZDnet, 1997); (Overly & Howell, 1998); (Terena, 2001); (Dixon, 1999); (Deloitte & Touche, 1997); (IEC, 2000); (Mackey & Gossels, 2000); (Certicom, 1997): private key (symmetric) encryption (e.g. Triple DES, IDEA, Blowfish, RC4, and RC5), and public key encryption (asymmetric) (e.g. RSA, SEEK, PGP, and ECC). The primary difference between the two methods is the number of passwords or "keys" that are used (Overly & Howell, 1998). “The central problem in most cryptographic applications is managing these keys and keeping them secret” (Baltimore, 1999).

Encryption mechanisms rely on keys or passwords. The longer the password, the more difficult the encryption is to break (IEC, 2000).

A symmetric key uses only one key to encrypt or decrypt a message; an asymmetric key uses two keys for encryption and decryption (Dixon, 1999); (Halsey, 1996). The symmetric encryption is faster, but the key is difficult to distribute securely. An asymmetric key is slower but a public key may be distributed. Public key cryptography replaces the secret key of symmetric encryption with a pair of keys (Baltimore, 1999); (Asokan et al, 1997); (Dfat, 2000), one private and one public. Information encrypted using the public key can only be retrieved using the complementary private key (Pei, 2001); (Martin1, 2000). This allows the sender of a message to encrypt it using the sender's private key. Any recipient may determine that the message came from the sender by decrypting the message using the sender's public key. For example, if a user called Alice encrypts a known piece of data, such as her telephone number, with her private key and transmits it to another user called Bob, Bob then decrypts the message using Alice's public key and compares the result to the known data. He therefore ensures that that the message could only have been encrypted using Alice's private key (Martin1, 2000).

With this system the public keys of all users may be published in open directories, facilitating communications between all parties. In addition to encryption, the public and private keys may be used to create and verify 'digital signatures'. These may be appended to messages to authenticate the message and the sender (Baltimore, 1999; (Asokan et al, 1997). PKI (discussed in 5.4.2 below) use public and private key encryption algorithm keys for encoding and decoding information (Dfat, 2000); (Asokan et al, 1997). Public key encryption is used for creating digital signatures and also to ensure integrity of a document. The transaction however may only be trusted if the total framework for supporting issue and maintenance of the keys is also trusted. "A widespread system of cryptographic keys will therefore inevitably lead to a need for a complex support system" (Asokan et al, 1997). This aspect is further discussed in Section 5.4.3.1 below.

These protocols also provide anonymity. Anonymity is desired, except that there must be some assurance that participants are who they claim to be. "Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authenticated" (VISA, 1997). For example before a user called Bob accepts a message with another user called Alice's digital signature, he wants to be

sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network. One way to be sure that the public key belongs to Alice is to receive it over a secure channel directly from Alice.

However, "security through encryption is never an absolute" (Hartman, 2001). All encryption is vulnerable to be broken, eventually. The key is to stay ahead of processing power and to limit the amount of information that be gained by cracking a single key. Technically speaking, there is a big difference between an algorithm and its implementation (Cobb, 1999). To quote leading cryptographer Schneier: "The technology is not weak in and of itself, it is just badly implemented" (Cobb, 1999).

This Internet connection needs to be made secure because of the Internet's public nature and the risk of fraudulent interception of private information. For effective use in electronic commerce situations, additional steps must be taken to make the web an acceptable medium (Dallas, 1998). To answer these concerns, two types of standard protocols have been developed (Le Tocq & Young, 1998); (Dixon, 1999); (Dallas, 1998) for securing the online purchase process:

- Secure protocols (e.g., Secure Sockets Layer (SSL), and Secure Hyper Text Transport Protocol (S-HTTP))
- Secure Payment protocols (e.g., Secure Electronic Transaction (SET) protocol)

These security protocols all use encryption techniques to provide adequate security (Zimits & Montano, 1998); (Le Tocq & Young, 1998); (Mehta, 1999), but "SET and SSL are targeted at different applications" (Zimits & Montano, 1998).

As described above, encryption forms the basis of many other controls as well and is used to ensure confidentiality and integrity. Secure protocols are also used in the digital certification process. The IS auditor needs to understand this technology and the role that it plays in the control process, because the control will be evaluated as part of the audit process (i.e. during the performance of the steps in the audit program).

5.4.1.2 Secure Protocols

SSL and S-HTTP are examples of general security- related protocols. There are other encryption methods such as IPSec and Tunneling that are also mentioned

below. Also, separate payment related protocols have been developed to handle financial transactions. Examples include SET (Secure Electronic Transaction), CyberCash and First Virtual. These will be further explained under the SET section in 5.4.1.2.2 below. Most of these protocols secure only the payment information such as the credit card numbers but not necessarily other information that may be confidential such as the customer order (Mehta, 1999).

Network transport security by default does not include encryption and strong authentication (Dixon, 1999). HTTP, FTP, and Telnet security features are generally limited to user identification and password authentication. Two methods of attack have been developed to compensate for the lack of security. The first is Virtual Private Networking (VPN) protocols to provide encrypted links between systems to extend internal networks and to connect with external systems, networks, and users. VPN is discussed below in Section 5.4.6. The second is Secure Transport protocols that use encryption to provide confidentiality and authentication between systems and applications. Network transport security is provided using one of five different protocols (Dixon, 1999). These are:

1. **IPSec (Ipv6)** - A network level protocol that is an enhancement of the TCP/IP protocol commonly used. IPSec encrypts network traffic and authentication from machine to machine. Its weakness is that it does not provide the granularity needed to connect individual users without additional controls that provide physical security and strong user authentication.
2. **Secure Socket Layer (SSL)** - The most popular protocol in use today (Dixon, 1999); (Pei, 2001); (CPG, 1999); (McDow, 2001). SSL is discussed in more detail in Section 5.4.1.2.1 below.
3 **Private Communication Technology (PCT)** - A technology introduced by Microsoft that mimics SSL v3.0 (Dixon, 1999); (Overly & Howell, 1998). PCT incorporates a separates authentication and key exchange providing stronger authentication keys.
4 **S-HTTP** - (Secure HyperText Transfer Protocol) An application layer transport method that provides for protected communication using Privacy Enhanced Mail. S-HTTP runs at the application layer of the OSI ISO standard. In other words, it stacks up at the same level as http. This protocol is flexible in terms of the type of encryption used. It includes private key, public key and message digests. S-HTTP is a security-enhanced variant of HTTP, which provides similar capabilities to SSL, and the two may easily co-exist in a complementary fashion by layering S-HTTP on top of SSL (Walder, 1999). S-HTTP is used to encrypt information that

has been entered into an HTML document by a client and sent to a server, or to encrypt information being sent by a server to a client (Dallas, 1998). S-HTTP is incapable of handling streaming voice and data, and it is not widely accepted (Dixon, 1999); (Dallas, 1998); (Mehta, 1999).

5 **Transport Layer Security (TLS)** - A protocol that is based on Netscape's SSL v3.0 and portions of Microsoft's PCT to create a standard security protocol (Dixon, 1999); (Overly & Howell, 1998). TLS has yet to be promulgated for use, and is still under revision.

The IS auditor needs to be aware that there are several different secure protocols in use and that secure protocols also play an important role in the controls identification and evaluation process. The IS auditor therefore needs to have an understanding of the role that secure protocols play in the controls process. Because SSL has been accepted as the most popular protocol in use (as shown in point 2 above), SSL will be discussed in more detail below.

5.4.1.2.1 Secure Sockets Layer (SSL)

The use of secure protocols is one way to enhance security (Mehta, 1999). SSL, developed by Netscape (Walder, 1999); (Zimits & Montano, 1998); (Pei, 2001); (McDow, 2001) is supported by the leading browser software such as Netscape and Internet Explorer from Microsoft (Walder, 1999); (Rapp, 2001); (ZDnet, 1997); (Overly & Howell, 1998); (Terena, 2001); (Pei, 2001); (McDow, 2001); (Sun, 1998). SSL is a protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP, offering data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection (Rapp, 2001); (Techguide, 2000); (Mehta, 1999); (Walder, 1999); (Dallas, 1998); (Pei, 2001). SSL uses public-key technology (Zimits & Montano, 1998); (Asokan et al, 1997); (Martin1, 2000); (McDow, 2001). SSL is a socket-layer communication interface that allows two parties to communicate securely over the Internet (Zimits & Montano, 1998); (Asokan et al, 1997). It is not a payment technology per se, but has been proposed as a means to secure payment messages. SSL does not support non-repudiation.

An encrypted SSL connection requires all information to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality (Pei, 2001); (McDow, 2001); (Martin1, 2000). Confidentiality is

important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering, i.e., for automatically determining whether the data have been altered in transit.

SSL is in common use today in many e-commerce servers, and offers "session-level" security (Le Tocq &Young, 1998); (Walder, 1999); (Dixon, 1999); (Mehta, 1999). This means that once a secure session is established, all communication over the Internet is encrypted, including the URL the client is requesting, any submitted form contents (including things like credit card numbers), any HTTP access authorisation information (user names and passwords), and all the data returned from the server to the client. This is also known as end-to-end encryption of data sent between web client and web server (Mehta, 1999). Additionally, since SSL encrypts everything (Le Tocq & Young, 1998); (Dallas, 1998); (Dixon, 1999); (Mehta, 1999), the display of complex pages may be slow, and therefore SSL protected sites often use minimal graphics to minimize the performance impact (Le Tocq & Young, 1998); (Dixon, 1999).

A SSL session is the equivalent of using a scrambler on the telephone line to the catalog merchant (Dixon, 1999); (Le Tocq & Young, 1998). When the data arrives at the merchant's web site, all the information is decrypted and whether or not it is stored in a secure format is the responsibility of the merchant: the user has no control over the security of their information and the data is only as secure as the host machine. (Le Tocq & Young, 1998); (Mehta, 1999); (Dixon, 1999); (Pei, 2001). The purchaser therefore:

- Has to trust that the merchant will guard their credit card information securely and the purchaser is assuming a risk in doing so (Dixon, 1999); Le Tocq & Young, 1998).
- Has no assurance that the merchant is authorized to accept credit card payment (Dixon, 1999); Le Tocq & Young, 1998).

SET (as discussed in 5.4.1.2.2 below) overcomes this problem. In an on-line transaction the merchant also suffers a security risk, as with any mail-order or telephone-order transaction, because he has no proof that the user is the true owner of the credit card (Le Tocq & Young, 1998); (Dixon, 1999); (Pei, 2001). This is a risk that the merchant and the credit card vendor assume and factor in to their cost of doing business. This risk increases with the purchase of "soft goods" and intellectual

property (software, games, etc.) where the purchase is actually delivered on-line as well as being ordered on-line.

The SSL protocol operates in two phases. In the first phase, the sender and receiver agree on the read and write keys to be used, and then in the second phase data is encrypted using the keys chosen (McDow, 2001); (Techguide, 2000). Authentication and secure key exchange is also achieved using the RSA public key encryption algorithm. At the opening of the SSL session there is a negotiation to determine the level of security (Martin1, 2000); (Pei, 2001); (McDow, 2001); (Mehta, 1999). The security level is determined by the 'weakest party'. The other one may consider the level as unacceptable and refuse the connection. For example, one party may only be able to cipher with 40 bits DES encryption and the other party does no accept less than 56. SSL users authentication allows a server to confirm buyer and supplier identity. SSL verifies that digital certificates are valid and have been issued by a certificate authority (CA) listed in the server's list (Martin1, 2000).

Here are the steps taken during a SSL transaction (McDow, 2001):

1. The client sends a request for a document to be transmitted using the S-HTTPS protocol by prefixing the URL with "https".
2. The server sends its certificate to the client.
3. The client checks to see if a trusted Certification Authority (CA) issued the certificate. If not, it gives the user the option to continue or to terminate the transaction.
4. The client compares the information in the certificate with the information it just received concerning the site: its domain name and its public key. If the information matches, the client accepts the site as authenticated.
5. The client tells the server what ciphers, or encryption algorithms, it can communicate with.
6. The server chooses the strongest common cipher and informs the client.
7. The client generates a private (or session) key using the agreed cipher.
8. The client then encrypts the session key using the server's public key and sends it to the server.
9. The server receives the encrypted session key and decrypts it with its private key.
10. The client and the server then use the session key for the rest of the transaction.

"Holes in SSL have already been identified, arising not from weaknesses in the underlying encryption technology, but from shortcomings in the implementation." (Cobb, 1999).

As shown above SSL is used in two of the major browsers used by users of the Internet. The IS auditor therefore needs to understand the importance of SSL as well as having a background understanding of how SSL works. The IS auditor also needs to be aware that the implementation of SSL creates weaknesses if it is not done correctly. The evaluation of the implementation controls will be performed as part of the audit steps.

5.4.1.2.2 Secure Payment Protocols

Secure payment protocols are usually independent of the transport protocols mentioned above in 5.4.1.2 and are network architecture independent. Secure payment protocols generally send encrypted data that requires a key in order for the merchant to complete the transaction (Dixon, 1999). Some of the more common secure payment protocols are:

1. **First Virtual** - A user has an account and receives a password in exchange for a credit card number, but the password is not protected as it traverses the Internet. "Such a system is vulnerable to eavesdropping" (Asokan et al, 1997). When the user makes a purchase, the vendor forwards the request to First Virtual (First) for authentication; First Virtual then queries the user to verify the purchase request. Upon acceptance by the user First Virtual then notifies the vendor of the successful transaction where upon the vendor sends the merchandise.

   First Virtual achieves some protection by asking the payer for an acknowledgment of each payment via e-mail, but the actual security of the system is based on the payer's ability to revoke each payment within a certain period. In other words, there is no definite authorization during payment. Until the end of this period, the payee assumes the entire risk. "This method is protocol independent and slow" (Dixon, 1999). "First Virtual is a cryptofree system" (Asokan et al, 1997).
2. **DigiCash** - Tokens are purchased from a bank or created by a user that is routed through a bank to guard against fraud. The token's amount is exposed

but the serial number is hidden. The transaction is complete when the token is accepted.

3. **Cybercash** – This protocol uses wallet software on the user's desktop that responds to the purchase request. The wallet software is activated when the vendor responds the sales data. It is routed to CyberCash where the ability to pay is validated for the user and the transaction completed. A major drawback is that the wallet is tied to one particular desktop.
4. **MilliCent** – This is ideal for buying and selling digital products costing from $1/10^{th}$ of a cent to $10 or more. Accounts may be opened directly with MilliCent or through a MilliCent broker. Funds are held in the account until needed and then spent at vendor websites with the click of a mouse. MilliCent takes care of the actual payment, the currency conversion, resolves content delivery problems and automatically processes refund requests. Users fund their accounts through an online debit or credit card, by billing their monthly ISP statement or telephone bill or through pre-paid cards purchased anonymously through convenience stores (MilliCent, 2000).
5. **Open Market** - A user issues a purchase request. The seller sends a "Digital Order" to the user where it is forwarded to a financial institution that verifies the ability to pay. The financial institution then forwards a digital request back to the seller. Buyers do not have to disclose the payment method (Dixon, 1999).
6. **Smart Cards** - Smart cards contain a microchip embedded into a standard plastic card. Information may be stored on a smart card, and software programs may be loaded and run on those cards with microprocessors. By storing digital certificates or a secret encryption key, smart cards may be used as identification cards, electronic cash, credit cards, remote access tokens, and storage of medical records (Zimits & Montano, 1998). Smart cards may also be a card issued with a fixed monetary value. The value is reduced with every transaction. The monetary value is tied to the card. The holder gets to use it. If the card is lost the monetary value is lost also (Dixon, 1999).
7. **Secure Electronic Transaction** (SET) - A protocol backed by MasterCard and Visa and supported by many other organizations that use Public Key Infrastructure (PKI) (VISA, 1998); (Dixon, 1999). The user makes a purchase request and the vendor checks with a payment gateway to verify the ability to pay. SET is discussed in more detail in 5.4.1.2.2.1 below.

   SET technology protects transaction information over open networks in four ways:

a. The cardholder is able to authenticate that a merchant is authorized to accept payment cards in a secure manner using SET technology.
b. The merchant is, in turn able to authenticate the payment card used in the transaction.
c. Advanced encryption technology protects personal payment information during transfer over the network.
d. Only the intended recipient may read payment information. Only the merchant and the financial institution using valid SET technology may read the information. As SET is distributed today, buyers are assured that the vendor is an authorized acceptor of the payment card. Merchants are assured that the user of the card is the authorized user of the card. SET offers a more secure form of purchasing for merchants because of the "client-side authentication". The merchant is assured that the purchaser cannot deny that they entered into the transaction process.

In summary, secure transactions must be considered in the light of competing goals depending on who is being considered. Customers want to protect their credit, credit card information and personal information from unscrupulous activity. The merchant wants to know who is buying their products, with assurance that they will be compensated for the purchase. Financial institutions want to protect against fraud and to increase the activity based on their particular financial infrastructure. The protection methodologies described depend upon public key infrastructures (PKI) for the validation and authentication of the participants in e-commerce transactions. The IS auditor therefore should understand that there are several different payment protocols available although some are more popular than others. One of the most well-known payment protocols is SET and SET is discussed in 5.4.1.2.2.1 below.

5.4.1.2.2.1 Secure Electronic Transaction (SET)

By using sophisticated digital certificates, SET makes the Internet a safe place for conducting business (VISA, 1997). SET focuses on authenticating the parties involved in a transaction, ensuring message integrity, and maintaining confidentiality of information (VISA, 1998); (Overly & Howell, 1998). The SET specification is an open specification available from several software and browser providers. SET duplicates and extends identification and authentication, while it adds authorization and repudiation (VISA, 1997). How these security aspects are addressed in SET, will be explained in more detail below.

SET is a system for ensuring the security of financial transactions on the Internet (Peixian, 2000); (VISA, 1998); (James, 1999); (Le Tocq & Young, 1998); (Pei, 2001); (McDow, 2001). It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others (Peixian, 2000); (VISA, 1988); (Zimits & Montano, 1998), (Walder, 1999); (Overly & Howell, 1998); (Terena, 2001); (Pei, 2001); (CPG, 1999). With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures between the purchaser, a merchant, and the purchaser's bank (Peixian, 2000); (Pei, 2001). The cardholder application or digital wallet is stored on the consumer's computer or Internet access device that also stores the card holder identity, digital key, and reference information from the card to be charged for the transaction (VISA, 1997).

SET provides confidentiality of payment and ordering information, since even the merchant never gets to see the customer's payment details, which are passed directly to the card company whilst still encrypted (Walder, 1999); (Dixon, 1999); (Overly & Howell, 1998); (Pei, 2001); (CPG, 1999); (McDow, 2001). This ensures integrity for all transmitted data, and provides authentication that a cardholder is a legitimate user of an account. The major advantage of SET over existing security systems is the addition of digital certificates that associate the cardholder and merchant both with a financial institution and the Visa or Mastercard payment system in a way that ensures privacy and confidentiality (Dixon, 1999); (Peixian, 2000); (Martin1, 2000) as well as non-repudiation (Martin1, 2000); (Dixon, 1999); (VISA, 1998); (James, 1999). Digital certificates provide the foundation for SET (McDow, 2001); (Walder, 1999); (CPG, 1999); (Pei, 2001).

SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP) as well as companies like IBM, Verisign, and American Express (Walder, 1999). SET uses some but not all aspects of a public key infrastructure (PKI) (Dixon, 1999); (Peixian, 2000); (Walder, 1999). With SET, merchants authenticate cardholders through SET certificates. According to VISA (1998): "Merchants can more readily accept credit cards without need for merchant-based credit card registration processes. And consumers only have to register their cards once with their financial institution to use SET at all participating merchants." Like the signature on the back of a credit card, digital certificates verify that the consumer is authorized to use a payment card and the merchant is authorized to accept it (VISA,

1998); (Dixon, 1999). The digital certificate is automatically sent from the consumer to the merchant as part of the order instructions (VISA, 1998). SET software automatically checks that the merchant has a valid certificate representing their relationship with their financial institution. "This provides consumers with the confidence that their payments will be handled with the same "Visa promise" of trust as used in credit cards" (VISA, 1998).

SET was designed to use public key encryption technology for credit card-based commerce on the Internet (Zimits & Montano, 1998); (James, 1999); (Dixon, 1999). According to James (1999): "In practice, banks will give both keys to a customer together with a digital certificate for authenticity. When customers wish to purchase over the Internet, they firstly give the public key to the merchant along with the certificate to prove its authenticity. Likewise, the merchant provides its own public key and certificates to prove its own bona fides to allow the transaction to proceed." Problems may arise in key distribution and customer identification while attempting to ensure that accounts and clients match (James, 1999); (Martin1, 2000); (Dixon, 1999). SET enables credit card transactions on the Internet by replacing every step in the existing processing system with an electronic version (Zimits & Montano, 1998); (Dixon, 1999). These steps are described as follows (Peixian, 2000); (James, 1999); (VISA, 1998); (Pei, 2001); (McDow, 2001):

1. The customer opens a Mastercard or Visa bank account.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been digitally signed by the bank to ensure its validity.
3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
4. The customer places an order over a Web page, by phone, or some other means (Peixian, 2000) (James, 1999).
5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment may only be used with this particular order.

7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
8. Then, the merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate. Next, the purse at the merchant's Web server sends a payment request to the consumer's purse (James, 1999). Thirdly, the consumer confirms the payment and sends a message to the merchant to clear the payment with the bank. The merchant's Web site then contacts the bank for confirmation that the purse is valid and has unspent funds. The bank then sends confirmation to the merchant's Web server and at the same time allocates the funds to a safe created on the bank's system for that merchant
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant, who may then fill the order.
11. Finally, the merchant software provides a receipt to the customer.

"Fortunately, this long-winded process is completed by modern on-line systems within a second or two" (James, 1999). Various layers of encryption are applied to protect these transactions. When a customer purchases funds from the bank, these are debited to the consumer's account, but after that, the use of the funds remains unknown to the bank, since they are submitted by the merchant, not the consumer, for reasons of privacy. "As typically implemented today, SET offers a much more secure purchasing process from the merchant's standpoint by using "client-side authentication" (Le Tocq & Young, 1998). This means that the merchant is sure that the purchaser cannot deny that they entered into the transaction.

Within SET, only the sensitive information in the transaction (name, address, credit card, etc.) is encrypted. When the consumer views the web pages, the pages are not encrypted as they travel to the consumer, enabling the web site designer to use graphics more liberally. An important point from a security angle is that SET is designed to protect only financial information, not electronic messages or other documents, so it is not subject to U.S. government export restrictions (Walder, 1999); (McDow, 2001). This means that SET-based systems will be able to incorporate full 128-bit encryption outside the USA and Canada.

SET may be used with SSL (Pei, 2001); (CPG, 1999). In such an environment SSL is used to communicate with customers, while SET is used at the back-end. This process will sidestep the need to deploy wallet software to customers. It provides the customer with merchant authentication, but not the merchant with consumer identification, as the consumer is not required to have an electronic wallet or digital certificate. SSL is designed to secure communications between a browser and a server. "However, most common usage of the Internet today is via browsers, and it has been suggested that SSL used in combination with LDAP can accomplish everything SET can without expensive software infrastructure upgrades" that are usually required for SET (Le Tocq & Young, 1998).

"The sluggish reception the market has given SET may indicate it is too complex and costly for current applications" (Zimits & Montano, 1998). "A downside of both SSL and SET is that they require the use of cryptographic algorithms that place significant load on the computer systems involved in the commerce transaction" (Le Tocq & Young, 1998). SSL has a lower impact on the e-commerce server but does less to eliminate the security risk. SET has a higher performance impact, but allows for a much more secure transaction. However, SET has its weaknesses: "its implementation is not as clean as the specification, so interoperability is an issue; it is complex and makes the transaction quite slow" (ECA, 2000), and some protocols, such as Secure Sockets Layer has taken the lead by integrating security directly into the browser.

The requirement to invest in additional hardware to support SET has been noticed in some early implementations, and some commentators have predicted that SET will not be able to cope (Le Tocq & Young, 1998); (CPG, 1999). "Many merchants are willing to take the risks inherent in SSL (which is true) and have not thought through the positive impact that can result if additional consumers are willing to participate when security is demonstrably high, or the risk of consumer confidence dropping when stories of fraud start to emerge" (Le Tocq & Young, 1998). Merchants are opting for a secure server environment that supports a larger traffic volume despite the larger risk. The performance impacts mentioned above have raised concern that despite its advantages in risk reduction, the SET protocol is impractical or too expensive to implement at today's required performance levels (CPG, 1999); (Le Tocq & Young, 1998); (McDow, 2001).

According to CPG (1999):

> "Another newly announced standard, the Electronic Commerce Modeling Language (ECML), may help make digital wallets - both SET- and SSL-based - more palatable to consumers. The standard, developed by a group of industry leaders, including Visa, MasterCard, Trintech and America Online Inc., aims to standardize the formatting of data in digital wallets and merchant payment systems. This would enable consumers to maintain one digital wallet rather than multiple wallets for different vendor sites, and would eliminate having to fill out a separate HTML payment form for every purchase. Trintech is supporting the standard in its new product, the ezCard, a JavaBeans-based virtual credit card that sits on a consumer's desktop and contains a digital certificate and personal ID from the issuing bank. What ECML allows you to do is issue virtual credit cards that are compatible with the payment forms at retailers."

The IS auditor should be aware of the payment protocols and the controls provided through the implementation of these protocols. SET is being used currently and is backed by the major credit card companies, so the IS auditor may come across SET as part of the audit of EC payment security. The IS auditor needs to be aware of the controls provided as well as the limitations and this will aid in the design and determination of the audit testing to be performed.

5.4.2 PUBLIC KEY INFRASTRUCTURE (PKI)

In Chapters 1 and 3 it was noted that lack of security is often cited as a major barrier to the growth of e-commerce, which can only be built on the confidence that comes from knowing that all transactions are protected by core functions. PKI is a mechanism for both authentication and encryption, combining software, encryption technologies and services to protect network communications and e-business transactions (PWC, 2000).

The following describe PKI and its importance.

- According to Mehta: "Public Key Infrastructures (PKI) are one of the ways businesses can deploy e-commerce from a security and authentication perspective." PKI comprises the processes and systems needed to effectively

manage digital certificates (Mehta, 1999); (PWC, 2000); (E-witness, 2001). "PKI is a system that provides the basis for establishing and maintaining a trustworthy networking environment through the generation and distribution of keys and certificates. This function can be performed internally or outsourced to a third party specialising in it" (Mehta, 1999); (PWC, 2000).

- Another argument for PKI is made by iStory, which states: "Public key technology is emerging as the cornerstone of the future business infrastructure, and a set of applications, policies, practices, standards, and laws will emerge from public key technology that are referred to as the public key infrastructure (PKI). It is the public key infrastructure that will serve as the arbiter of security and trust on the Internet, ultimately unleashing its economic potential" (Zimits & Montano, 1998).
- "A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust" (Baltimore, 1999).
- In order to employ public-key based security solutions one often needs an infrastructure for secure user registration, public-key certification, and directory services. Usually this is called PKI (Peixian, 2000).
- In Public Key Cryptography (as discussed in 4.1 above), each user is given two key pairs, one pair to encrypt/decrypt messages and one to sign/verify them. In PKI, these are issued as digital certificates by the Certification Authority (CA) who acts as a trusted third party and who vouches for the digital certificates they issue. "But public key cryptography, on its own, is not enough if we are to truly re-create the conditions for traditional paper-based commerce in an electronic world. Security experts generally agree that Public Key Cryptography and the adoption of a Public Key infrastructure (PKI) are today the best available means of providing the highest level of security on the Internet" (Sinnreich et al, 1999).
- Yet another argument for the use of PKI to address Internet security risks is made by Verisign (1999): "One element has now emerged as the foundation for secure distributed applications, including supply chain management, secure messaging, e-commerce, virtual private networks, and intranet applications – that element is Public Key Infrastructure (PKI). An enterprise's PKI constitutes the core of its Internet security infrastructure. The success of an enterprise's PKI will have a major impact on core business operations." The foundation for secure Internet applications is a Public Key Infrastructure (PKI)."

- "PKI is becoming the cornerstone of many organisations' security strategy" (Globalsign, 1999).

From the above statements the conclusion is made that PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the desired levels of protection of assets (including information). This objective is achieved through the five principle security functions for commercial transactions mentioned earlier in this chapter and briefly repeated below.

- **Confidentiality** - To keep information private and ensure that information is not intercepted during transmission (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000).
- **Integrity** - To prove that information has not been manipulated (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000); (E-witness, 2001).
- **Authentication** - Validating the identity of parties or applications in communications and transactions through digital certificates (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000).
- **Non-repudiation** - To ensure that information cannot be disowned, and ensuring that transactions, once committed, are legally valid and irrevocable (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (Martin1, 2000); (E-witness, 2001).
- **Availability** – Ensuring that transactions or communications may be executed reliably upon demand (Verisign, 1999); (Baltimore, 1999).

According to the above definitions, Public Key Infrastructure therefore consists of the following building blocks and key components:

- **Encryption algorithms** - The basic mathematical algorithms used to scramble information. Symmetric (private) encryption uses the same keys to encrypt and decrypt, whereas asymmetric (public) encryption uses separate keys to encrypt and decrypt information. This was described in 4.1 above.
- **Private and public keys** - A secret private key and a mathematically related public key are generated for each party in a transmission. Given the public key, it is nearly impossible to determine the private key. This was described in 4.1 above.

- **Digital signatures** - An electronic signature that is irrefutable, unique, and virtually impossible to copy or transfer. PKI is based on digital IDs known as 'digital certificates', which act like 'electronic passports', and bind the user's digital signature to his or her public key. (Baltimore, 1999). Digital signatures are described in more detail in Section 5.4.3 below.
- **Digital certificates** - An electronic document comprising a public key, digital signature, owner identity, serial number, issuer, and expiration date. This is described in 4.3 below.
- **Certificate Authorities** (CA) - Issuers of digital certificates acting as a "trusted third party" in electronic transactions (Zimits & Montano, 1998); (Baltimore, 1999); (Jones, 2001). This is described in Section 5.4.3 below.
- **Security Policy** - defines the rules under which the cryptographic systems should operate (Baltimore, 1999); (Martin1, 2000). This is briefly described below as well as in Section 5.4.7.1 below.
- **Registration Authority** (RA) (Baltimore, 1999); (Jones, 2001). This is described in Section 5.4.4 below.
- **Certificate distribution system** including repository, revocation system, generation, registration, and certification (Baltimore, 1999); (Mehta, 1999); (Martin1, 2000). This is described in Section 5.4.3 below.
- **PKI-enabled applications** (Baltimore, 1999). This is described below.
- **Procedures** to dictate how the keys and certificates should be generated, distributed and used as described in the Certificate Practice Statement (CPS) of a CA (this is also described in more detail below).

As indicated, the PKI components of security policy, CPS, and PKI applications is described in more detail below:

- **Security Policy**

  A security policy defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography (Baltimore, 1999). Typically it will include statements on how the organisation will handle keys and valuable information, and will set the level of control required to match the levels of risk. Other aspects of the security policy are described in more detail in Section 5.4.7 below.

- **Certificate Practice Statement (CPS)**

  Some PKI systems are operated by commercial Certificate Authorities (CAs) or Trusted Third Parties, and therefore require a CPS. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users (Baltimore, 1999). In other words, a CPS explains the practices CAs employ when issuing certificates, the security it employs to protect its own environment and the legal rights and obligations of the CA and those who rely on its certificates (Wilson, 1999); (Sun, 1998); (Stewart, 1998).

  According to Feindt & Culpin (1998): "VeriSign Inc is an example of a CA providing digital ID/certificates for "trusted electronic commerce. VeriSign's Certification Practices Statement (CPS), a 107-page website document is accepted by the end-user during the registration process (probably without careful reading)." "A CA's trustworthiness remains essential to digital signature authentication" (Stewart, 1998).

  There are differences between the USA and Europe regarding the regulation of CAs. According to Feindt & Culpin (1998): "A Memorandum of Understanding from European Industry therefore recommends a non-regulatory approach: the development of a set of guidelines regarding the operating procedures of the CAs, reflected in Certification Practice Statements. The establishment of trusting relationships between the CAs could be handled by an industry-led body which oversees the EU guidelines for Certification Practice Statements." The US favours a non-regulatory approach relying on private initiatives. For Europe, under the common framework for electronic certification services proposal, data authenticated with an electronic signature issued by an accredited CA may be used as evidence at court in the same manner as if the data had existed in a manually signed form (Feindt & Culpin, 1998).

- **PKI-enabled applications**

"A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits" (Baltimore, 1999).

Examples of applications are:

- Communications between web servers and browsers (Baltimore, 1999); (Jones, 2001).
- E-mail (Baltimore, 1999); (Jones, 2001).
- Electronic Data Interchange (EDI).
- Credit card transactions over the Internet.
- Virtual Private Networks (VPNs) (Baltimore, 1999); (Jones, 2001).

Although PKI has been described above as an important factor in EC security, the auditor also needs to be aware that there are certain shortcomings to PKI. "Like any new, business-critical technology, the evaluation and implementation of a PKI solution is a challenging and intricate process, which requires a great deal of planning, management and clear guidance" (Baltimore, 1999). "Its effectiveness has been hampered however by the fact that several PKIs are in use, and no standard yet exists" (PWC, 2000). "Although many companies have started implementing this, PKI is in its infancy. Besides lack of industry standards, the PKI itself needs infrastructure" (Mehta, 1999).

However, the following conclusion is made:

> "It is easy to get caught up in the mathematical complexity of public key encryption and lose sight of the fact that the public key infrastructure is about much more than technology. The PKI is best thought of as a framework of accepted business practices and legal statutes supported by systems and software. The PKI resolves the fundamental problem of trust in the Internet. Providing strong privacy, authentication, data integrity, and non-repudiation, the PKI fulfills fundamental security requirements. A great deal of time and attention has been devoted to heralding the economic potential of the Internet – it is the Public Key Infrastructure and the trust it adds that will realise that potential" (Zimits & Montano, 1998).

To summarise, technically, PKI refers to the technology, infrastructure, and practices needed to enable use of public-key encryption and/or digital signatures in distributed applications on a significant scale. The main function of PKI is to distribute public keys accurately and reliably to those needing to encrypt messages or verify digital signatures (used to sign transactions or to authenticate people prior to granting access to resources). This process employs digital certificates issued by an enterprise CA to users who register with that CA. Issuance of a certificate requires authentication of the user, usually by a RA. The scope of PKI also extends to functions such as certificate renewal, certificate revocation/status checking, and user private key backup/recovery. Digital certificates will be discussed further in Section 5.4.3 and CAs in Section 5.4.3.1 below.

PKI includes many of the components important in the controls process of EC payment security. The IS auditor needs to understand what components make up a PKI and evaluate the individual PKI components relevant to the EC payment security audit to the extent to which the component serves as a control to minimise the risk.

5.4.3 DIGITAL CERTIFICATION

Digital certificates and signatures have been mentioned above as one of the key components of PKI. Digital certificates and signatures will be described in more detail below.

Digital certificates are used to endorse an electronic document in a way that may be later validated for authenticity. The CA that endorses a server's Web site certificate uses these. This process aids achieving non-repudiation (Martin1, 2000); (Mehta, 1999); (Walder, 1999); (Zimits & Montano, 1998); (Asokan et al, 1997); (ZDnet, 1997); (Feindt & Culpin, 1998); (Jones, 2001); (Scit, 1998); (Yasuda, 1997).

Digital certificates are like electronic fingerprints that positively authenticate the identity of the person or Web site (Martin1, 2000); (Mehta, 1999); (Feindt & Culpin, 1998). The certificate itself is simply a collection of information to which a digital signature is attached (PWC, 2000); (Mehta, 1999); (Walder, 1999). The digital signature is attached by a CA, a third party authority that is trusted by the community of certificate users (Walder, 1999); (Zimits & Montano, 1998); (Asokan et al, 1997); (Terena, 2001); (James, 1999); (Pei, 2001); (Certicom, 1997). By electronically

signing a digital certificate, a CA vouches for the certificate owner's identity. The main function of a digital certificate is to validate the public key of an individual or network device (e.g., to validate content) (Zimits & Montano, 1998); (Dixon, 1999).

Typically, the digital certificate includes the unique name of the owner; name of the CA who is vouching for the identity of the certificate holder; a unique serial number; the period of validity of the certificate, and a digital key (Mehta, 1999); (Mackey & Gossels, 2000); (James, 1999); (Pei, 2001); (Yaacov, 1997). CA's will also be discussed in more detail in Section 5.4.3.1 below. However, digital certificates may also contain information that defines user privileges, and so play a role in managing access control.

Before understanding digital certificates, knowledge of digital signatures is essential. When combined with message digests, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message (or document) that is unique to that message. A message digest is generated by passing the message through a one-way cryptographic function; that is, one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message (Martin1, 2000); (Mehta, 1999); (Dekker, 1997); (Widman, 1999). The algorithm used by SET generates 160-bit message digests. The algorithm is such that changing a single bit in the message will change, on average, half of the bits in the message digest. It is computationally unfeasible to generate two different messages that have the same message digest (Martin1, 2000); (Mackey & Gossels, 2000). The message digest is signed using the CA's private key to create a message authentication code (MAC). The MAC may be verified by anyone processing the CA's public key (Halsey, 1996); (Asokan et al, 1997).

It may be proved that the transaction originated from a particular source (authentication), since certificates are based on the sender's private signing key, and authenticated by the public verifying key (Walder, 1999); (Dekker, 1997); (IEC, 2000); (Baltimore, 1999), but it may also be proven that the transaction has not been tampered with in any way during transit (i.e., integrity), since any tampering after signing invalidates the signature (Dekker, 1997); (Walder, 1999); (Kabay, 1998); (Norton, 2000); (Martin1, 2000); (Widman, 1999); (Scit, 1998); (IEC, 2001); (Baltimore, 1999). This is done by decrypting the digital signature using the originator's public key, and comparing the result with a summary produced by

passing the received message through the same mathematical function (Martin1, 2000); (Scit, 1998). "While it sounds complicated, in practice the entire process can be as simple as selecting an icon on a computer screen" (Martin1, 2000).

Public key cryptography makes digital signatures possible (Martin1, 2000). As with encryption, digital signatures may make use of either secret key (where both parties require copies of the same shared key), or public key (with a public/private key pair) methods. The public key methods – such as DSS and RSA – are more popular since key management is very much more straightforward (Walder, 1999); (Asokan et al, 1997). Digital Signature Standard (DSS) provides electronic signature capabilities to Federal agencies and departments (Halsey, 1996). It was developed for use by companies that do business with the US Government and is a signature-only system, whereas RSA may be used both for signing and generally encrypting a message (Walder, 1999). An example of the use of a digital signature is provided by VISA (1997).

> "Alice computes the message digest of a property description and encrypts it with her private key yielding a digital signature for the message. She transmits both the message and the digital signature to Bob. When Bob receives the message, he computes the message digest of the property description and decrypts the digital signature with Alice's public key. If the two values match, Bob knows that the message was signed using Alice's private key and that it has not changed since it was signed."

The portability and scalability of a digital certificate supports a wide variety of applications. For example, digital certificates and private encryption keys may be issued using various media depending on the level of assurance required (e.g., smart cards) (Zimits & Montano, 1998); (James, 1999); (Sinnreich et al, 1999). Those issued only on smart cards or other certified security tokens provide the highest level of user and server security/identification for electronic commerce and are used for high value transactions. Those issued on diskettes or stored on hard disks are used for lower-value transactions and authenticated access to online services. Over time, digital certificate-configured smart cards will likely become the standard for credentials such as passports, driver's licenses, and credit cards (Zimits & Montano, 1998).

As shown in the above description on digital certificates, they are used to secure confidentiality, authentication, non-repudiation, and integrity of EC payments and are therefore regarded as an important control to consider for the IS auditor. IS auditors need to understand the role that digital certificates play in the EC payment security process so that when they design an audit approach, this control may be included where required.

5.4.3.1 Certification Authority (CA)

Certification authorities hold a central role in the PKI by acting as the repository of trust from which digital certificates derive legitimacy. Digital certificates are created, managed, administrated, and revoked by the CA. "Much like the government issues and guarantees the identity of the passport bearer, a CA acts as the guarantor of the validity of the digital certificate" (Zimits & Montano, 1998).

A CA is a trusted entity (Mehta, 1999); (Walder, 1999); (Zimits & Montano, 1998); (James, 1999); (Overly & Howell, 1998); (Stewart, 1998) that provides the function of an independent third party to authenticate the identity of the Web site or person (Sun, 1998); (Certicom, 1997); (Yaacov, 1997). "It is important that the CA is trusted in order that the certificate can be considered genuine" (Walder, 1999). A system is needed to authenticate the identity of public key holders, as otherwise, illicit organisations might distribute sham public keys among users (James, 1999). In order to be able to get this service, companies must register with the CA. Applications of certificate authorities range from private companies administrating network privileges to broad-scale electronic commerce linking suppliers and manufacturers (Zimits & Montano, 1998); (James, 1999) and government affiliates (Zimits & Montano, 1998). Virtually any transaction requiring proof of identity or validation of privileges provides an opportunity for a CA to act as a trusted third party. Probably the best know CA at the moment is VeriSign (Walder, 1999); (Feindt & Culpin, 1998), though other systems such as IBM's World Registry, GTE's CyberTrust and Nortel's Entrust have also been introduced (Walder, 1999); (ZDnet, 1997); (Mackey & Gossels, 2000).

The CA will use its private key to place its digital signature on the certificate. When a user hits over an SSL session, the certificate of registration is downloaded to the user's browser. The signed certificate is decoded using the public key of CAs stored in the browser software. If the decoded information matches the information in the

browser, the web site is authenticated. "However, CAs only help in authentication. This does not necessarily mean that the Web site can be trusted in terms of the types of goods and information that are sold" (Mehta, 1999).

The creation of a PKI involves integrating public key technology with law in order to form a "trusted" infrastructure suitable for commerce activity. In the USA, more than 50% of states have digital signature laws or are in the legislative process to create digital signature laws. Other countries include Germany Malaysia, etc. (Zimits & Montano, 1998). "A public CA must understand how to coordinate its policies and procedures with existing domestic and international laws. Additionally, a well-formed policy with prescribed practices and formal auditing is fundamental to operating as a public CA" (Zimits & Montano, 1998).

As things progress, it should be possible (and desirable) to have a hierarchy of CAs, going from banks or reputable organisations at the bottom, all the way up to government bodies and even, perhaps, a global controlling body such as the United Nations. "This means that if you don't trust the first CA you can check the certificate on its digital signature with the next CA up the tree, and so on up the hierarchy until you reach the "root" CA" (Walder, 1999).

When implementing a PKI, an organisation may either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party. "While installing a server and other components of a CA system are well within the reach of most companies' information technology teams, the primary challenges lie in management and policy, not cryptography and systems" (Zimits & Montano, 1998). The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle (Baltimore, 1999); (Jones, 2001); (Certicom, 1997); (Zimits & Montano, 1998). Unique elements to a CA system's operations include:

- Key management.
- Certificate validation.
- Issuing certificates by binding the identity of a user or system to a public key with a digital signature.
- Scheduling expiry dates for certificates.
- Ensuring certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs).

- Key updates.
- Key recovery.
- Policy administration and maintenance.

Central to a CA system's flexibility are its use of directories (Zimits & Montano, 1998); (Baltimore, 1999). Directories are similar to databases, however, directories are primarily used for reading information rather than transactions or complex queries. In a CA system, directories are used to store and distribute digital certificates, keys, cross-certification lists, entries for distribution of certificate revocation lists (CRLs) and to retrieve keys. "An open CA system must be able to perform these basic functions and most importantly, support individual customisation in order to meet security requirements while achieving business objectives" (Zimits & Montano, 1998).

"Perhaps the thorniest issue facing all CA systems is the life-cycle management of digital certificates" (Zimits & Montano, 1998). One element of management is validation. It is important to be able to determine if a certificate is valid at any given time. CAs are responsible for providing the current status of any digital certificate they have issued. For example, a CA within a company will experience new hires, changes in employee privileges, lost passwords, and employee departures. In all circumstances, the digital certificate directory must be updated to accurately reflect these changes. "While publishing a new certificate is relatively straightforward, certificate revocation and validation are more challenging" (Zimits & Montano, 1998).

The X.509 standard is the most commonly used standard for certificates (Walder, 1999); (ZDnet, 1997); (Halsey, 1996); (Halsey, 1996); (Yaacov, 1997). Certificates based on the X.509 standard incorporate an expiry date to ensure that old certificates are revoked automatically after a given period of time. However, there also needs to be a system in place to allow certificates to be revoked before expiration time (e.g., the private key or CA signature is compromised) (Levi & Koc, 2001); (Fratto, 2000) or immediately in certain cases – say where a certificate (perhaps contained in a smart card) has been stolen. The X.509 standard defines what information may go into a certificate and describes how to write it down (Sun, 1998). This includes the version, serial number, issuer name, validity period, public key information, certificate ownership, etc. This provides for complete "non-repudiation", whereby digitally signed messages may be proved authentic to a third party, thus allowing such transactions to be legally binding. Certificates are given a set life span when issued

e.g., a certificate may be valid for one year. Then it expires and a new certificate must be issued. According to Fratto (2000) "there is an indirect relationship between the information contained in a certificate and its useful lifetime. The more information in the certificate, the shorter its usefulness, because information may change and a new certificate will have to be issued before it expires.

Electronic commerce requires that certificates be validated each time they are used, in the same manner that credit cards are authorized. CAs validate certificates using three methods (Zimits & Montano, 1998); (Genuity, 1998):

- certificate revocation lists (CRLs),
- online certificate status protocol (OCSP), and
- certificate revocation trees (CRTs).

Certificate revocation lists are simply lists containing all certificates that are no longer valid (including certificates revoked before their scheduled expiration date (Zimits & Montano, 1998); (Halsey, 1996); (Apacheweek, 2000); (RSA, 2001); (SSE, 2001); (Levi & Koc, 2001); (Fratto, 2000). Each CA ideally maintains and updates the list in a timely fashion so anyone may check a digital certificate against the list and validate a certificate issued by a CA (Zimits & Montano, 1998); (SSE, 2001); (La Macchia, 2001). For small scale applications this works well. "But for geographically dispersed organizations with several hundred thousand employees or far-flung Internet commerce transactions, CRLs can quickly scale to an unmanageable size" (Zimits & Montano, 1998). Updated CRLs are made available according to the policy of the organisation (i.e. the CA). Expiration is checked against the most recent list.
The more critical an application's security requirements are, the more important real-time certificate validation becomes. For example, delays in updating CRLs in large monetary transactions such as settlements and funds transfers create credit risk. Other alternative methods of validation (i.e. CRT and OCSP) seek to address the problem of updating CRLs.

Online Certificate Status Protocol (OCSP) is meant to provide real-time validation for certificates (Zimits & Montano, 1998); (Levi & Koc, 2001); (Globalsign, 1999). While real-time validation makes sense, OCSP is an early stage standard (Zimits & Montano, 1998). Currently, an IETF working group has defined methods for using OCSP with the http protocol. Other protocols, such as ftp or smtp, are currently in discussion. "While OCSP does not address all concerns regarding scalability and

performance, in our view, real-time validation will be indispensable for large scale business-to-business electronic commerce" (Zimits & Montano, 1998).

"One method offering relief from update delays and scalability is the CRT model for certificate validation developed by ValiCert. Hash functions reduce any size message to a fixed length as well as confirming data integrity (e.g., a 15k byte number may be reduced to a unique 20 byte number)" (Zimits & Montano, 1998). Using these properties of hash functions, ValiCert's patent-pending method hashes the serial numbers of revoked certificates and reduces the volume of validation data as well as verifies the integrity of the revocation tree.

Another alternative in the use of CAs is to also use a Registration Authority (RA). An RA provides the interface between the user and the CA (Baltimore, 1999); (Jones, 2001). It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that is placed in the certificates. An RA therefore performs some of the functions that a CA will perform if the RA and CA combination is not used.

Where digital certificates are used, a certification authority is also required. The IS auditor needs to understand the role of the CA and the validation of certificates. These are important aspects to control the security of EC payments and an understanding of the role of the CA and certificate validity, expiration and control is important to the IS auditor when determining the audit approach and the testing to be performed.

5.4.3.1.1 Key Recovery/Escrow

Communications agencies require access to data for the purposes of system recovery after failure. Since all transmissions may have the same key, the agencies may wish to keep a register of private keys. Some governments propose that a copy of every private key be held in trust by national security agencies for their use in criminal investigations (James, 1999); (Abelson et al, 1998).

Key escrow is a system to provide encryption of user traffic, such as voice or data, so that the session keys used are available to properly authorised third parties under special access circumstances (James, 1999); (Abelson et al, 1998). Law enforcement agencies promoted the concept while other uses might be for recovery

of encrypted data following its loss or destruction due to equipment failure (James, 1999); (Abelson et al, 1998). The United States "Escrowed Encryption Standard" involved a computer ('Clipper') chip with a unique identity number and a two-piece secret key stored by two different agencies. However, users may already backup keys and there is no guarantee for liability or that any escrow agency itself is trustworthy. "However, key backup is useful for good management reasons in applying to archival data" (James, 1999).

Initial proposals for Key Recovery are based around "Key Escrow", also known as "Trusted Third Party" (Walder, 1999); (Abelson et al, 1998). There are a number of implementations of this, each of which involves providing a Key Recovery Centre (KRC) with the means to decrypt your encrypted sessions. One way this could work, for instance, is to provide the KRC with copies of your private keys. Another method is to embed the keys used to encrypt the message within the message itself in a "Key Recovery Field". This is then encrypted using yet another public key provided by the KRC, whilst the corresponding private key remains known only to the KRC.

In all implementations, however, the theory is that KRC's may only be forced to recover keys on presentation of a court order, thus protecting the interests of end users. "At the moment, products incorporating Key Recovery can make use of one of three proprietary, dynamic key management protocols – Internet Security Association/Key Management Protocol (ISA/KMP) Oakley (backed mainly by Cisco); Simple Key Exchange Internet Protocol (SKIP), backed by Sun; and Photuris Session Key Management Protocol, backed by Radguard" (Walder, 1999).

Key Recovery has been criticised by most of its likely users due to the potential for the criminal element to target Key Recovery Centres in an attempt to gain access to thousands of sets of data in a single swoop (Walder, 1999); (Abelson et al, 1998). To the hacker, KRCs represent an extremely valuable single point of failure for the system as a whole, made worse by the proposal that some KRCs would use a single key for many users (Walder, 1999). "There is also the feeling, of course, that it does not make commercial sense to allow any third party – even a "trusted" one – to hold keys which could provide access to sensitive corporate data" (Walder, 1999).

The IS auditor should be aware that there are many risks involved in key recovery/ escrow solutions, as well as to what extent the risks may be controlled. The controls

evolve around third party reliance and here the IS auditor may have to rely on the work of other IS auditors if access to the key recovery third party is not available.

5.4.4 FIREWALLS

Firewalls are relatively simple and very effective combinations of software and hardware that act as a barrier to protect an enterprise's perimeter (PWC, 2001); (Dekker, 1997); (Mika et al, 2001); (IEC, 2000). Firewalls separate internal systems from external systems (e.g. the Internet) (Lindner, 2001); (PWC, 2000); (Landrum, 2001); (E-witness, 2001); (Tyson, 2001); (Stewart, 1998); (Deloitte & Touche, 1997) and control the flow of communications in and out of the enterprise. They create a shield between the secure environment inside the system and the open potentially hostile external environment (Landrum, 2001); (Widman, 1999); (Stewart, 1998). A firewall is a device or system that enforces an access control policy between two networks (Cott, 2001); (Lindner, 2001); (Norton, 2000); (PWC, 2000); (Landrum, 2001); (Hartman, 2001). In principle, the firewall provides two basic services: (1) blocks undesirable traffic, and (2) permits desirable traffic. A firewall provides a single point of entry into a corporate network from an un-trusted network (i.e. the Internet). It is at this 'choke point' (Cott, 2001); (Hartman, 2001) that the access control policy and auditing capability are enforced.

The job of a firewall is to examine data as it enters the network and to block traffic that doesn't meet specified criteria (Jones, 2001). There are several types of firewalls and all may be used in combination and each has strengths and weaknesses depending on the needs and uses. The types of firewalls are (PWC, 2000); (Tremblay, 2000);(Landrum, 2001); (Hartman, 2001); (Techguide, 2000); (Jones, 2001); (Tyson, 2001); (Mika et al, 2001); (Deloitte & Touche, 1997); (Mahadevan, 2001); (Scit, 1998):

- Proxy server.
- Packet filter.
- Application gateway/ dynamic packet filter.

5.4.4.1 Proxy server

A proxy server is a firewall implemented in a hardware unit such as a workstation on a NT server, rather than in a router (Techguide, 2000). A proxy server performs several functions:

- Eliminates direct contact between a trusted resource and an un-trusted user and therefore acts as the middle-man between an un-trusted resource and a resource located within the trusted network (Jones, 2001); (Tyson, 2001); (Lindner, 2001); (Dekker, 1997).
- Hides the identities of resources within the protected network (PWC, 2000); (Dekker, 1997).
- Provides additional authentication and auditing capabilities (Dekker, 1997).

This device looks at all of the data in each packet, not just address and headers (Techguide, 2000), (PWC, 2000). In most cases, the proxy examines the content and replaces the network address in the packet with proxy destinations that are known to be secure (Techguide, 2000); (Mahadevan, 2001). Besides hiding the network from the outside world, they provide more control over the actual data at the application level. However, because they inspect all of the data in each packet, there have been reports of some significant performance degradations in high traffic areas (Techguide, 2000); (Jones, 2001).

5.4.4.2 Packet Filter/Screening router

A packet filter examines data packets entering and leaving the network and grants (users are known by their IP address) or denies them access to specified applications (determined by their port address) on the basis of specific criteria/filters (Tyson, 2001); (PWC, 2000); (Mika et al, 2001); (Stewart, 1998); (Mahadevan, 2001); (Mackey & Gossels, 2000); (Cott, 2001); (Techguide, 2000); (Tremblay, 2000); (Dekker, 1997); (Zwicky et al, 2000). This limits the connections of even those users allowed to enter through the firewall, and completely denies any connections to those not authorised to access any applications. These are also called network level firewalls. They are fast and transparent to users, but also the easiest to penetrate and are especially prone to "spoofing" attacks (Stewart, 1998); (Deloitte & Touche, 1997); (Mahadevan, 2001).

Routers may be used to filter packets as well (Cott, 2001); (Scit, 1998). This device would only be used to filter data and should not be considered a first line of defense. The main function of a router is to use header information and forwarding tables to determine the best route for packets to travel.

5.4.4.3 Application Gateway/ Dynamic Packet Filter

Authenticating Servers are often used in conjunction with Screening Routers to provide authentication (Techguide, 2000). According to Tyson (2001) this "does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded." An application gateway secures specific applications. Security mechanisms are applied when a connection is established; after that, network traffic flows without further checking (PWC, 2000). All packets are addressed to an application on the gateway that relays the packets between the two communication points. In most application gateway implementations, additional packet filter machines are required to control and screen the traffic between the gateway and the networks (Techguide, 2000). Typically, this is a use of bastion hosts (Techguide, 2000); (Deloitte & Touche, 1997). These are secure but inefficient, since they are not transparent to users and applications. According to Mackey & Gossels (2000) "they determine whether information is correctly formatted and decide whether it should be allowed or denied to the network."

The term "firewall" has become a generic term, which encompasses a spectrum of technologies intended to provide protection from communications attacks on an organization. It is possible, and often desirable, to combine these different technologies according to the needs of the organization and their budget limitations (Techguide, 2000); (Stewart, 1998).

Audit considerations for firewall security include:

- Avoiding remote firewall administration, especially over the Internet (Mehta, 1999) (Hartman, 2001). The firewall also needs to be securely managed to limit the

possibility of someone breaking into it. As the protector of the network, the firewall is a target for intruders. "Managing the firewall via the Internet interface is probably the least desirable situation, especially if the management connection is of questionable encryption strength or can be spoofed" (Hartman, 2001). Taking care not to allow management ports to be available to the Internet also helps prevent fingerprinting the type of firewall used.

- Upgrading firewall software on a regular basis with patches and upgrades (Hartman, 2001). Firewall software is like anti-virus software: effectiveness goes down over time as new vulnerabilities are discovered (Mehta, 1999); (Landrum, 2001); (Deloitte & Touche, 1997); (Mahadevan, 2001). For software-based firewalls, this applies to the operating system and the firewall software (Hartman, 2001).
- Having the firewalls reviewed periodically (Mehta, 1999); (Mahadevan, 2001). There are a number of commercial products that may help make this task easier such as the Internet Security Scanner ISS - http://www.iss.net. "Another alternative is to have knowledgeable information systems auditors help in this process" (Mehta, 1999).
- Improper configuration (Landrum, 2001); (Hartman, 2001); (Dekker, 1997); (Mehta, 1999) and not monitoring and auditing logs (Landrum, 2001); (Tremblay, 2000). The firewall product will deny access to unauthorized connections and show where those attempts originated and what ports they were dispatched to. There are many types of firewalls that may exist on the host. There are also firewalls that are used to protect networks. Information gathered from logs can be used to find patterns, misconfigured equipment and break-in attempts. This information can be used to communicate those attempts to the owners of the originating hosts.
- As with most operating systems Firewalls never come out-of-the-box configured to secure any given site and are only as good as the staff administrating them (Landrum, 2001); (Mehta, 1999).
- Filters should also be as specific as possible. Permissions for inherently dangerous traffic, such as rules that allow remote management, should always be as specific as possible. But less obvious threats are often overlooked (Hartman, 2001).
- "If you have different systems for your web site and your mail, don't just allow web and mail traffic to the entire subnet. Specify mail traffic allowed to the mail server and web traffic to the web server" (Hartman, 2001).

- Allowing SMTP traffic to a web server may not seem to be all that large a risk, but it is an unnecessary one (Hartman, 2001), i.e., evaluate whether SMTP traffic is needed.

It's important to note that in the Internet-enabled business environment, firewalls alone are no longer sufficient to provide all of the levels of security that are needed (Symantec, 2000); (Jones, 2001); (Deloitte & Touche, 1997); (Lindner, 2001). "Firewalls are not very effective at screening for viruses and cannot protect the network against attacks that do not go through it. Industry statistics show that a majority of security breaches originate from internal sources unseen by the firewall" (Lindner, 2001). Firewalls will not protect the network from vulnerabilities introduced by a lapse in security-consciousness by the user community (Lindner, 2001). Other levels of security needed include internal access control, encryption, backup and recovery, audit, logging and monitoring, and these aspects are also discussed in this chapter.

Firewalls are generally very effective at keeping unwanted people out of enterprise networks. They do this by establishing what types of network connections will be allowed and what session services will be supported. This works well when the boundaries of the network are clearly defined.

As shown above, firewalls are an important component used in EC payment security. Although the audit of a firewall may be considered for an independent review based cn the time required to ensure that the firewalls are properly controlled, the auditor involved in EC payment security audits should consider the controls over firewalls as part of the EC payment security review.

5.4.5 INTRUSION DETECTION SYSTEMS (IDS)

"As the use of the Internet as a cost-effective transport mechanism increases, so does the need for a real-time, automated intrusion detection and reporting capability" (Lindner, 2001). Since the paper trail in e-commerce is limited, it is critical to detect, prevent or at least limit intrusion to systems and data (Martin1, 2000). Firewalls and authentication servers act as 'passive' deterrents to unauthorised access to network and computer assets. However, in the event that a hacker is not deterred, network and computer assets are immediately at risk. "In many cases, a breach will not be detected until the damage is done and the hacker is long gone" (Lindner, 2001).

"Another layer may be to deploy an IDS system" (Tremblay, 2000). IDS may generally be configured to give you much more information than a firewall. They may also be set up to perform some action based on rules that are set for the IDS. The entire packet may also be captured to review later. Software applications or hardware devices known as an Intrusion Detection System (IDS) automate this process (Landrum, 2001); (PWC, 2000). IDS, like firewalls and other mechanisms mentioned, have limitations. Intrusion detection is therefore defined as the process of monitoring a network to identify, alert operators, or even take some action on network-based attacks or malicious activity (Tremblay, 2000); (Landrum, 2001); (Cott, 2001); (Hartman, 2001); (Dekker, 1997); (Mahadevan, 2001). An IDS provides a wide range of monitoring techniques including packet sniffing, file integrity monitoring, and even algorithms that detect deviations in network traffic. Real-time intrusion detection and reporting systems are 'proactive' deterrents, constantly scanning the network for suspicious activity and automatically logging and terminating those activities before any damage may be done (Lindner, 2001); (Cott, 2001); (PWC, 2000).

There are three approaches to intrusion detection: network based; host-based or a hybrid of the two approaches (PWC, 2000); (Norton, 2000); (Tremblay, 2000); (Jones, 2001). Each of these will be addressed below.

- **Network-based Intrusion Detection** is advantageous because it detects threats and attacks before they reach critical systems (Norton, 2000). "Agents or sensors are typically placed along the perimeter of the network behind firewalls and other access points to detect unauthorized activity that may compromise the perimeter defenses" (Norton, 2000). Network agents may also be placed on subnets in order to scan traffic that may cross the backbone. Placing agents or sensors in front of perimeter devices has the added advantage of detecting probes and attacks that may be stopped by the perimeter devices, and provides substantial information as to the value and effectiveness of those devices. Network-based systems "sniff" the wire, comparing live traffic patterns to a list of known attacks (Hartman, 2001); (PWC, 2000). According to Hartman (Hartman, 2001): "The problem is, if the signature-matching strategy is too specific, any small change by the attacker will allow it to slip through without detection. On the other side, if the signatures are too general, then there are many false alarms that desensitize the user. Striking the right mix is generally difficult and time consuming."

- **Host-based Intrusion Detection** detects threats and attacks on critical systems that may not be detectable by network-based systems including file access and encrypted transmissions (Norton, 2000). Host-based agents may be better than network-based agents at capturing user identifiers (Norton, 2000). Critical systems should be identified and protected (PWC, 2000). Host-based systems use software "agents" that are installed on all servers and report activity to a central console.

  Both methods (network or host based) require a regularly updated list of known attacks, just like anti-virus software. But they also detect an electronic attacker trying different password combinations and alert the operations center or even automatically shut down that part of the network. Neither (network or host based) system is able to detect all known threats and attacks.

- The most effective method is to **combine the two** into a real-time system that detect known attack signatures and patterns, as well as suspicious activity, including probes of the network or critical systems and unauthorized attempts to modify access control mechanisms (Norton, 2000); (PWC, 2000); (Dekker, 1997); (Jones, 2001). The system should be configurable to provide for immediate and automated alerts to such activity, and provide for configurable actions such as logging and automatically terminating the session (Norton, 2000); (PWC, 2000). Immediate and tactful response is necessary in the event of a threat, attack, system compromise, or misuse of network resources. An Incident Response Team should be formed and trained to respond to an identified security event. Automated response capabilities should be incorporated whenever possible (Martin1, 2000).

Tools for intrusion management therefore will include: use of monitoring software, the results of which are checked within a specific time-frame; automatic timeout; trends analysis; bench-marking; survey of markets for latest detection tools, patches, and anti-virus (Martin1, 2000), as well as a system wide audit program. A system-wide audit program should be implemented to provide for immediate and full logging of activity to enforce / achieve user accountability (Norton, 2000); (Martin1, 2000). A central repository for the audit logs will provide immediate and historical reference for an investigation or management request for information. The program should also include security and statistical analysis tools to evaluate the audit logs. The audit

program should include procedures to verify the integrity of individual systems and for compliance with existing system and security policies and procedures.

The IS auditor must be aware of the technology and the level of control provided by IDS, but must also be aware that IDS may be a strong addition to security and should never be deployed as a stand-alone solution. IDS should be considered as complementary to defense provided by the firewalls, border, host-protections, etc., not as a replacement for them. IDS must be considered in the design of the audit approach as it provides additional control when it is combined with other technologies mentioned in this chapter.

5.4.6 VIRTUAL PRIVATE NETWORKS (VPN)

VPN technology provides the medium to use the public Internet backbone as an appropriate channel for private data communication (Peixian, 2000); (Tyson2, 2001); (Rademacher & Tunstall, 1998). With encryption and encapsulation technology (Peixian, 2000); (PWC, 2000); (Hartman, 2001), a VPN essentially establishes a private passageway through the Internet (Jones, 2001); (Mika et al, 2001).

VPNs will allow remote offices, company road warriors, and even business partners or customers to use the Internet (Peixian, 2000); (PWC, 2001), (Rademacher & Tunstall, 1998) rather than pricey private lines, to reach company networks. So the companies may save a lot of money (Techguide, 2000); (PWC, 2000); (Peixian, 2000); (Zwicky et al, 2000). "This differs from credit card and consumer ordering transactions in that the volume of data between the two parties is greater and the two parties are well known to each other. This means that complex and proprietary encryption and authentication techniques can be used since there is no pretense to offer universal connectivity through this channel" (Cobb, 1999).

According to Hartman (Hartman, 2001):

> "This usually takes advantage of an encryption algorithm with a scheme to regularly exchange keys and can mask all traffic traveling through the 'tunnel'. The only thing visible to anyone on the Internet is encrypted data between the two VPN end points: all the services used, source / destination addresses utilized, and the data is hidden. An attacker is left without some of the clues that can help determine which traffic is valuable and which is not. All traffic would

have to be decrypted, hopefully at great expense, in the hope that some of it is valuable."

According to Tyson (Tyson2, 2001) "a well designed VPN should incorporate: security, reliability, scalability, network management, and policy management." A VPN should use several methods for keeping a connection and the data secure (Tyson2, 2001); (Rademacher & Tunstall, 1998), amongst others:

- **Firewalls** – firewalls may restrict the number of open ports and the packets and protocols allowed through. Firewalls were discussed in Section 5.4.4 above.
- **Encryption** – encryption was discussed in detail in Section 5.4.1 above.
- **IPSec** – IPSec was mentioned in Section 5.4.1.2 above. IPSec is a secure protocol that provides enhanced security features such as better encryption algorithms and comprehensive authentication and integrity checking. (Tyson2, 2001); (Rademacher & Tunstall, 1998).
- **Tunneling** – VPNs rely on tunneling to create a private network that reaches across the Internet. Tunneling is the process of placing an entire packet within another packet and sending it over the network. The protocol of the outer packet is understood by the network and by the points where the packet enters and exits the network.

The IS auditor should be aware that VPNs provide another alternative to EC payment security control. VPNs in turn use other technologies already described in this chapter (e.g., encryption). When designing an audit approach, the IS auditor must therefore be aware of the control provided by a VPN, and include the evaluation of the VPN as part of the overall control solution where applicable.

5.4.7 CLIENT-SIDE AND WEB SERVER VULNERABILITIES

According to AARF (AARF, 2000): "Highly secure cryptographic systems will fail to make significant improvements in security if they operate within an insecure IT infrastructure, which fails to address the basic security issues. Management considers the security infrastructure before evaluating the effectiveness of other security measures."

One of the obvious risks to Web servers as highlighted above is the denial of service attacks. Another issue is related to confidentiality of information that may be stored on Web servers or areas that are accessible by Web servers, such as database servers. If proper controls are not in place, this information could be retrieved, manipulated or destroyed.

Many security weaknesses of Web servers come from configuration issues, because typically, when installing the system, whether it is the firewall or the operating system, by default, a number of network services and protocols are made available. The more services available, the more routes a hacker or cracker will have to penetrate the internal private network.

Components of e-commerce security and controls include documented policies and procedures, thorough top management understanding and support of security, competent (and satisfied) employees and regular monitoring for compliance with standards. The aspects of policies, physical security, server controls, and other related controls will be discussed below for consideration by the IS auditor when the possible control to secure EC payments is considered.

5.4.7.1 Policies

Effective security starts with the development and implementation of a security policy (PWC, 2000); (Techguide, 2000); (Cott, 2001); (Norton, 2000); (de Beaupré, 2001); (Symantec, 2000); (Lindner, 2001). The establishment of security policies is the critical first step in protecting vital enterprise information assets. These policies may also be used as a defense against potential legal liabilities. "Today enterprises must define or redefine their security policies to include rules regarding Internet access and acceptable use" (Symantec, 2000). "The security objective and core principles provide a framework for the first critical step for any organisation developing a security policy. The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organisation" (IFAC, 1998). A good policy unifies all aspects of your security measures into a single strategy and establishes an enforceable set of rules (Dekker, 1997). "Technical controls such as firewalls and IDS are only part of a properly developed security program" (de Beaupré, 2001). The security process is all about applying the appropriate policies through proper procedures and management practices.

According to Lindner (Lindner, 2001): "A security policy establishes the rules or protocol under which the entire organisation or company will be required to operate. The protocol established in an organisation's security policy must be incorporated into the daily habits of every employee. The policy is backed up by an ISO 17799-based standards or procedures document that specifies the access control requirements for information and other assets throughout the company." A security policy needs to lay out, in writing, the security processes of an organisation, and outlines the issues of who, what, when, how, and why of ongoing actions and procedures. It should be a detailed document that identifies risks, defines steps taken to reduce them to acceptable levels, and outlines the tasks and job-descriptions of those directly involved in the enforcement of security in an organisation. According to Hartman (Hartman, 2001) "it is both a checklist and a shield." The checklist portion forces the organisation to ensure it has performed due diligence to create a secure environment. It is also a shield because it outlines people's roles and responsibilities so that they may point to the document to show legitimacy and direction to their actions.

Formal security policies and security standards documents should be tailored specifically for each networking environment. The documents must be distributed to every employee throughout the organisation and be an integral part of an ongoing security education and awareness program (Lindner, 2001); (Pethia et al, 1991). Periodic assessment of systems, policies, and procedures provide for effective augmentation of existing security programs, and the implementation of new security measures and countermeasures (Martin1, 2000); (Mackey & Gossels, 2000).

As described above, security policies are the foundation of effective security and the IS auditor should understand the security environment of an organisation and ensure that aspects related to EC payment security are also covered in the policy. Adherence to the policy should be evaluated by the IS auditor as part of the detailed audit tests.

5.4.7.2 Physical Security

Setting up the best, most-expensive, highest-technology network security is a waste of time and money if access to equipment is not controlled (Hartman, 2001); (Nim, 1998). "If the information is valuable enough to steal, then physical security needs to

be up to the task." (Hartman, 2001). A really solid network defense is not complete if someone may physically gain access to equipment or private networks. Equipment should have several layers of physical security (Hartman, 2001); (Unixtools, 2001). Controlled access to the building, a secure network room, locked cabinets for the equipment, and maybe a screen to prevent wireless communications from leaving the room are examples of considerations for physical security. E-commerce servers must also be located in a secured building. Physical security aspects should be specified in the policies and procedures documentation (Martin1, 2000). "Allow only appropriate physical access to computers" (CERT, 1999).

Apart from the physical security aspects mentioned above, consideration should also be given to business continuity planning. Disaster Recovery procedures may be invoked if the severity of the event is high enough to require it. This could result from the destruction of a critical system through an intentional or unintentional event. It may also happen as the result of a natural disaster. Any plan in place should address specific e-commerce needs. Plans should be benchmarked with plans of other similar organisations or environments. Backups should be tested regularly for recovery purposes (Scit, 1998) and stored off-site (Unixtools, 2001). Unlimited Power Supply (UPS) should be used to provide backup electrical power in case of a power failure that affects the computer site and network.

Security Assessment is a tool that may be used to improve security on an ongoing basis. This requires detailed analysis of detected events and their responses lead to continual refinement of the controls. System weaknesses are identified for re-fortification, false positives are eliminated, and thresholds are revised. Security awareness programs are enhanced. This monitoring aspect will also assist the IS auditor to obtain information on possible problems in the security environment. Aspects such as physical security is important to the IS auditor as they form part of the baseline of controls in an organisation i.e., if the basic controls such as environmental controls are not present in an organisation, then the detailed controls over applications such as EC payment systems may be circumvented. The auditor therefore needs to evaluate the basic controls as part of the overall assessment.

5.4.7.3 Server Controls

Securing the Operating System (OS) and Web service is very important (Landrum, 2001). Once it has been compromised, attacks into internal systems are possible.

There are numerous considerations to secure an OS and Internet/web server. Many of these issues have been mentioned in other sections of this chapter. The points below refer specifically to the web server and the operating system issues. Where applicable, the area in this chapter where the issues have been mentioned will be noted below. Areas to consider include:

- Removing default CGI scripts that are not needed -- these are typically not meant for commercial use. (Mehta, 1999); (CERT, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- The web server should utilize the minimum privileges to execute CGI scripts (for example, on a UNIX system, a web server should not execute as 'root'). (Mehta, 1999); (CERT, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Automatic directory listing should be turned off. If this is available, the program sources could be downloaded for examination for potential vulnerabilities. (Mehta, 1999)
- Disabled acceptance of SSIs (Server-Side Includes). SSIs are codes embedded within HTML documents. If these are uploaded to the web server they will execute under the web server privilege. (Mehta, 1999); (Ghosh, 1997).
- Restrict the directories from where CGI scripts are executed from the web server. This is because if CGI scripts are placed in user directories, there could be security threats (Mehta, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Check for proper configuration of cookie distribution. Cookies are sent between a web server and client. This could include authentication information. If the cookies are misconfigured, an unauthorized server might be able to retrieve that cookie, and in theory, could then try to gain unauthorized access to the original web server (Mehta, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Check to ensure all deadly defaults for the specific application and supporting operating systems are addressed. In order to find out information on the deadly defaults, one may visit the CERT sites (http://www.cert.org), vendor sites, and other security related sites such as http://www.ntsecurity.net for Windows NT. (Mehta, 1999); (Dekker, 1997); (Unixtools, 2001); (Interhack, 1997).
- Turn off network services that are not needed. If the server is a mail server, http and ftp may not be needed. Opportunities for attacks increase with the number of enabled network services. (Mehta, 1999); (Mackey & Gossels, 2000); (CERT, 1999).

- Keep up with the latest operating system (OS) patches. These typically address potential security related OS bugs and holes that have been discovered. (Mehta, 1999); (Interhack, 1997) (Dekker, 1997); (CERT, 1999); (Unixtools, 2001); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Use of strong passwords (Landrum, 2001); (Hartman, 2001); (Dekker, 1997); (Terena, 2001); (Pethia et al, 1991); (CERT, 1999); (Unixtools, 2001). Weak passwords feature on the SANS Institute top-ten vulnerabilities list. (Martin1, 2000) Standard controls should apply, such as regular reviews of policies, password length and format, frequent forced change of password (e.g., every 30 days), access rights linked to staff movement, unique identifier, regular audit of the effectiveness of the procedures and applications by staff. This was also discussed in the authorisation section.
- Only installing services that are needed – as discussed in the firewalls and DoS sections (Mackey & Gossels, 2000).
- Document what is installed and monitor for any changes - DoS section.
- Run logging and monitor log files (Landrum, 2001); (Hartman, 2001); (Pethia et al, 1991). Actions of users should be logged and reviewed. (Dekker, 1997); (CERT, 1999).
- Limit open ports to required needs – network services (Fuller, 2000); (Todd, 2000); (PCIS, 2000); (CERT, 1999).
- Block the ability to know OS and web server information (Mackey & Gossels, 2000); (Landrum, 2001).
- Limit access to the system. (Landrum, 2001); (Hartman, 2001); (Unixtools, 2001) Proper authentication techniques are vital. This comes down to having users log onto the system with their own user IDs (never directly as root or administrator) and care being taken to ensure proper authority levels are granted. Different authentication schemes may be utilized such as Kerberos, Radius or LDAP but it comes down to enforcing logins with proper privileges and enforcing strong password usage. Care should also be taken in how a login is achieved. Remote connections across the Internet that use a non-secure medium should always be avoided as they could be easily captured and read (such as telnet) (Landrum, 2001); (Hartman, 2001). DoS section and authentication.
- Keep the system up to date with latest fixes and patches. (Landrum, 2001); (Hartman, 2001); (Cobb, 1999); (Pethia et al, 1991); (CERT, 1999); (Unixtools, 2001). Keep up to date on Bugtraq or CERT advisories, and apply the necessary

patches to ensure there is no exposure to any newly discovered vulnerabilities. (Dekker, 1997); (Mackey & Gossels, 2000). DoS section.

- Image, ghost, or back up the system at appropriate stages (Landrum, 2001); (Scit, 1998); (Martin1, 2000); (CERT, 1999). Backup is mandatory as more reliance is placed on the electronic audit trail. Organisational requirements should dictate the backup policy and this should be coordinated closely with a disaster recovery plan - www.interhack.net - Physical security section,
- Stage and test applications and systems on a staging server prior to implementation of systems, applications or changes in a production environment (Landrum, 2001),
- Change default configurations that may endanger security i.e. customise the operating system to the environment where it is implemented (Mehta, 1999); (Cobb, 1999); (Mackey & Gossels, 2000) – DoS section.

Web network traffic should be separated from the internal network (CERT, 1999); (Landrum, 2001). This isolates the less secure systems from the more secure making it difficult for an attacker to pick up or sniff internal traffic for valuable information. Using a firewall as previously discussed will do this. Another option is to put all database and file servers providing web support service on a protected subnet. It is also important to disable any source routing that will allow the originator to influence routing decisions.

One component often overlooked in all the various security models, methods, and protocols, is the end user's computer (Rapp, 2001). No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end users' computer. That computer has stored all the digital certificates, most of the consumers' personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers, which store information in some very basic forms, even plain text. This use means the consumers' financial and banking data is only as secure as that computer. To further complicate matters, there are many lap top computers used at home and in business. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data. Controls that minimise this risk are physical security and policies as described above.

Other important considerations to address vulnerabilities on the client or web server site include change management; managing direct connections to server; regular

reviews; reconciliation; audit trails; exception reporting, etc. It is not the intention to describe each of these aspects in detail as most aspects may be considered separate areas of audit to an IS auditor. The IS auditor needs to be aware that there are other aspects that could pose a risk to the audit of EC payment security and the results of the audits in the areas mentioned should be considered together with the EC payment security audit. This is required to evaluate the impact on the exposures and to determine whether other controls being evaluated may be strengthened to address those issues. These areas may be addressed by the IS auditor as they pertain to the EC payment security audit.

- **Change management** - There should be approval processes for upgrades and for the implementation of new systems, as well as control over the segregation of duties between the development staff and operational staff and a separate logical development and production environment.
- **Privacy assurance involves** tools that seek to ensure confidentiality, integrity, authenticity and non-repudiation. These are usually achieved through compliance certificates and independent audits.
- **Regular reviews** will provide Quality Assurance that all controls are working effectively. (Martin1, 2000).
- **Reconciliation** control is achieved through independent reconciliation of e-commerce transactions through adequate segregation of duties. (Martin1, 2000).
- **Audit / paper trail** - It is not feasible to envisage that a totally paperless system will have all the key controls to ensure that an adequate audit trail is maintained (Martin1, 2000). Documentation is critical as the paper trail is reduced. (Martin1, 2000). Whatever management decides is critical should be secured in hard copy form. An electronic audit trail must have the ability to follow a transaction from end-to-end and identify all critical steps. Testing of the audit trail should ensure that any errors/ irregularities could be promptly identified and corrected. (Martin1, 2000).
- **Exception reports** - Reports should be concise and should focus on critical activities. They must be in a format that allows prompt monitoring of the e-commerce activities highlighted in the report. (Martin1, 2000).

As soon as technology is developed to address vulnerabilities, new vulnerabilities tend to be identified. Thus, keeping up with security issues is always challenging.

The technologies mentioned above are all used in the effort to address the six major risk areas as mentioned in Section 5.3 above as well as in Chapter 4 of this study. These are all possible controls and it does not necessarily imply that all the above technologies will be present in all organisations that take part in EC payments. The IS auditor needs to understand the impact of the use of these technologies on the control environment. With an understanding of the available technologies, the IS auditor will be equipped with the necessary knowledge to develop an audit approach to EC payment security. This approach is dependent on the specific environment being audited.

5.5 CONCLUSION

As described in this chapter, the seven elements of a secure business environment are access control, authentication, availability, data privacy/ confidentiality, integrity, non-repudiation, and web/client side controls. Each is a necessary component for a complete solution. This chapter identified the technologies available to control each of the elements mentioned above.

When the IS auditor encounters electronic commerce activity on the Internet, the auditor needs to determine the sensitivity of the transactions. Transactions that contain confidential or sensitive information should be protected from unauthorised disclosure or alteration – usually through some form of encryption. Transactions that should create concern for the auditor are those that involve payments, shipment of goods, or commitments for services.

No system will, however, be one hundred percent secure. Measures are available to be taken to minimise the possibility of a successful attack. Detection, prevention, and reaction are the measures that do this. Securing a system is therefore the implementation of minimum controls necessary to protect the system with an acceptable degree of assurance.

The audit of the security of EC payments is not a single task or subject but involves many different technologies that need to be taken into account. As discussed in this chapter, many of the technologies aid in securing EC payments. The role of the auditor is to understand the available technologies, assess the risks of implementing the technologies and identify the controls required to ensure that the technologies will provide the assurance required. When the IS auditor understands the available

technologies and the controls provided by these technologies, this enables the development of an audit approach.

CHAPTER 6

AN AUDIT APPROACH TO E-COMMERCE PAYMENT SECURITY

INDEX

6.1 INTRODUCTION

As stated in Chapter 1, the purpose of this dissertation is to develop an audit approach for the IS auditor that can be used when an IS auditor is involved in the audit of an e-commerce (EC) payment security environment. The previous chapters addressed the following:

- The role of an auditor with specific reference to the IS auditor (Chapter 2);
- The EC payment security environment (Chapter 3);
- The risks prevalent in this environment (Chapter 4), and
- The possible controls to mitigate the identified risks (Chapter 5).

These chapters provide a basis for the audit approach which the IS auditor may follow when auditing EC payment security.

The purpose of this chapter is to present the audit approaches followed by other audit organisations, and translate the commonalities in these approaches into steps that the IS auditor should follow as part of the audit approach to EC payment security.

This chapter is structured as follows:

1. Firstly, an acceptable audit approach is defined by highlighting the approaches of the major external, public audit and accounting firms, as well as other internal audit department approaches;
2. Secondly, the audit steps to be followed are identified as part of the audit approach; and
3. Thirdly, an overview is provided regarding the considerations and audit procedures that should be taken into account and/or carried out when the IS auditor performs an audit in the EC payment security environment. Detailed considerations are provided in Appendix A of this dissertation.

6.2 AUDIT APPROACH

6.2.1 A DEFINITION OF AUDIT APPROACH

The *Roget's Thesaurus* defines "approach" as "a method used in dealing with something" (Roget, 1980). *Webster's Dictionary* (Merriam-Webster, 1988) defines "approach" as "the taking of preliminary steps toward a particular purpose" or "a particular manner of taking such steps".

The following definition of an audit approach is provided by Abrema (2002): "The audit approach refers, in broader terms, to the manner in which evidence is to be gathered and evaluated".

Although other references to the topic are later referred to, the above two definitions clearly point out that an audit approach indicates the manner or method of performing an audit and it includes certain steps that need to be taken in order to achieve a certain end result (i.e., the completion of the audit).

6.2.2 ELEMENTS OF AN AUDIT APPROACH

6.2.2.1 Audit Approaches from Major Accounting Firms

The audit approaches of the major Audit and Accounting firms were chosen for further analysis because the approaches of these organisations should reflect the standards and practices of the Auditing profession. According to Businessmajors, (2002); Rutgers, (2002); iBig5, (2002); CSU, (2002); Emich, (2002); EIU, (2002); USD, (2002); Accountantsworld, (2002); the major audit and accounting firms (also known as the "Big 5") are considered to be:

- Arthur Andersen;
- Deloitte & Touche;
- Ernst & Young (EY);
- KPMG, and
- PricewaterhouseCoopers (PwC).

The audit approaches followed by these five major public audit and accounting firms are defined below.

The Arthur Andersen approach is defined as follows:

"Our audit approach is risk-based. Together with management, we identify the key business and accounting risks you face. We then test controls in place to mitigate those risks. This approach focuses attention on relevant areas, generates value-added recommendations, and ensures an effective and efficient audit process" (Andersen, 2002).

Deloitte & Touche (Deloitte, 2001) state: "we will identify the areas of risk associated with the industry as well as the potential errors relevant to the specific organisation being audited. We will design appropriate audit procedures that focus on these risks."

The key features of the EY audit approach are (EY, 2002):

- "Focus on key business risks – the methodology is designed to more closely align our audit process with your underlying business risks,
- Emphasis on controls – using a controls based approach, we evaluate and when appropriate, test the effectiveness of internal controls.
- Analytical and data analysis procedures – using our increased knowledge of your business, our greater focus on your business risks, we use analytical and data analysis procedures to provide audit evidence from which we gain significant audit assurance or identify areas requiring further investigation."

The audit approach used by KPMG (2000) consists of 5 elements, each of which includes the identification of risk issues:

1) "Strategic analysis – understand the internal and external forces which impact business. This highlights the high level risks and management control framework.
2) Business Process Analysis – assess the impact of key processes and the risks if they do not perform. It also allows the identification of performance measures and controls in place.
3) Business measurement – assess how well key business processes are controlled against targets.

4) Risk assessment – review key risks identified, which impact the business and financial statements.
5) Continuous improvement – identify improvement ideas."

The approach by the Information Risk Management section of KPMG (KPMG, 2002) states:

"The foundation of the IRM internal audit approach is an assessment of business risks.

- What role does information technology play in achieving the client's business objectives?
- What are the risks to the organization if information technology does not support those objectives in a cost-effective manner?
- What are the risks to the organization if its information technology systems are inadequately controlled?

The IRM methodology seeks answers to those questions, thereby ensuring a cost-effective and client-appropriate solution."

The PricewaterhouseCoopers (PWC) audit approach is "risk based and exceptions orientated" (PWC, 2001).

6.2.2.1.1 Summary of the Audit Approaches of the Major Accounting Firms

From the above examples from the "Big 5" accounting firms, it is clear that the preferred audit approach is risk-based, which is summarised in the following steps:

- Scope and understand the environment;
- Identify the risks, and
- Identify the controls to address these risks.

Additional steps (e.g., for the reporting process) are not addressed here as this is not unique to an IS audit. Once the audit environment is understood, the risks and possible controls, including the nature and extent of audit procedures, have been identified, what remains is performing the audit tests, evaluating the findings, and reporting on the findings. The process is iterative as well: e.g., where testing reveals

other risks that need to be addressed, the new risks then need to be included in the full audit approach cycle.

6.2.2.2 Audit Approach as Prescribed by Professional Organisations

The EDP Auditors Foundation developed an "Information Systems Audit Approach" based on that of the American Institute of Certified Public Accountants (AICPA). This approach defines a step-by-step audit approach for information systems. It involves the following steps (EDPAA, 1983):

- Scope and understand the environment – determine what technology is used and the way the technology influences the audit process. This is done to provide the auditor with sufficient background to conduct the audit;
- Identify the audit risks – identify areas of audit concern and determine where to most effectively focus the audit efforts and resources;
- Identify audit evidence – this will help to establish the base for conducting audit tests;
- Identify key control points – identify the controls to address the risks identified above;
- Identify control weaknesses – this will help to focus testing on areas where the probability of error is the highest;
- Conduct the audit tests, and
- Conclude the audit.

The approach of the IS auditor to an audit, including an audit of EC payments security, is also defined by professional organisations such as the Information Systems Audit and Control Association (ISACA1, 2001) and the South African Institute of Chartered accountants (SAICA, 1998) as follows:

- Gather information related to the area being audited;
- Identify the risks prevalent in the environment being audited;
- Identify possible controls that should be implemented to mitigate the identified risks;
- Develop an audit approach to serve as a framework for the area under review.

This approach is also followed in Guidance Statement AGS1056 (AARF, 2000) with reference to Electronic Commerce risk and control considerations, as well as the International Auditing Practice Statement on Electronic Commerce (IAPC, 2001).

These steps are designed so that they are inter-dependent. The output of each step will serve as the input of the following step. For example, the controls identification process cannot take place effectively without the risks being identified.

From the audit approaches followed by the professional organisations as highlighted above, it is clear that they correspond to the approaches followed by the major accounting firms (as identified in 6.2.2.1 above).

6.2.2.3 Audit Approaches Followed by Other Organisations

The following are examples of individual internal audit departments' audit approaches:

- A risk based audit approach is used by Suffolk (Suffolkacct, 2002). It involves the following four steps:
  - determine the threats,
  - identify the control procedures that should be in place to minimise each threat,
  - evaluate the control procedures,
  - evaluate weakness (errors and irregularities not covered by control procedures).
- The audit approach used by the ParkHill Audit Agency (Parkhill, 2002) is to "utilise a risk based auditing approach, which involves highlighting key controls and evaluating and testing them accordingly".
- "Our audit approach assesses risk for each source independently, providing the focus to address differing levels of risk. We offer our clients a value-added audit approach which is flexible, innovative and proactive" (CPGCA, 2001).
- Mossadams' audit approach involves "evaluating the risks you face on a daily basis. We use our understanding of your business to design an effective and efficient audit process. We are value-driven and seek to maximize the return on your investment in the audit process through in-depth analysis of your financial statements, your internal controls, and your business. We provide value-packed

management letters that address issues such as operational efficiency and how you can strengthen internal controls" (Mossadams, 2002).

- The audit approach used by Moorestephens (1997) is defined as follows: "The basis of our audit approach is a close understanding of the operations of the entity, its systems and controls, and the business environment in which it operates. The knowledge gained during our audit assignments is useful in assisting our clients to improve their systems, controls, and profitability."
- Another approach is defined by an internal audit Association in the United Kingdom (Internalaudit, 2001). This approach involves the following steps:
  - Carry out a risk and control overview and report on the results. The report suggests an estimated total number of audit days required per cycle. This exercise is valuable in its own right;
  - Agree on a detailed work plan, listing individual assignments to be carried out in each year of the cycle, and the number of days allocated to each assignment;
  - Carry out work in accordance with the plan, notifying heads of department in advance of each assignment;
  - Clear findings and recommendations with managers;
  - Produce a draft, and later final report in the format chosen by the client;
  - Follow up the status of previous audit reports;
  - Attend periodic review meetings, including audit committee meetings.
- The approach followed by Soberman (2002) is defined as follows: "Our audit approach remains risk-based. This means that we get rapidly to the heart of the issues that affect our clients and their financial statements as a whole. We then plan our audits to focus timely and sufficient attention on identified risk areas. We continue to focus on clients' systems and internal controls in order to identify controls that are effective and relevant, and that can be tested efficiently. In addition, we support management in fulfilling their responsibility to safeguard assets and ensure the efficient operation of their organization."
- The NHSD (2002) approach is defined as follows: "Our risk-based audit approach improves the overall efficiency of the engagement by working with key personnel to identify and mitigate risk to an agreeable level".
- The Internal Audit department of Robert Patrick & Co (Robert Patrick, 2002) uses an approach of:
  - Reviewing operations to assess risk;
  - Developing an internal audit program;

- Conducting the internal audit program.
- Reporting findings to senior management.

- The approach used by the Tufts University (Tufts, 2002) "utilises a best practices approach by providing recommendations to management that will reduce high internal control risks and business liability exposures."

From the above statements it is clear that there are commonalities in the approaches used by the major external audit and public accounting firms and individual company internal audit departments. These common steps are subsequently used in this dissertation to define the audit approach to be followed when auditing EC payment security. The common steps are identified in Section 6.3 below.

6.3 COMMON STEPS IN THE EC PAYMENT SECURITY AUDIT APPROACH

The audit approaches followed by the major accounting firms, professional organisations, and other organisations, as highlighted above, clearly indicate that the approaches are very similar in nature. From these approaches the following steps summarise the audit approach. (This excludes the steps related to the audit testing and reporting functions as each audit requires the inclusion of audit tests and reporting on results as part of the approach. The purpose of this dissertation is to highlight the approach for aspects unique to the EC payment security environment):

1. Scope and understand the environment – determine what technology is used and the way the technology influences the audit process. This is done to provide the auditor with sufficient background to conduct the audit;
2. Identify the audit risks – identify areas of audit concern and determine where to most effectively focus the audit efforts and resources;
3. Identify audit evidence – this will help to establish the base for conducting audit tests;
4. Identify key control points – identify the controls to address the risks identified above;
5. Identify control weaknesses – this will help to focus testing to areas where the probability of error is the highest.

In addition to the above steps, two other elements also affect the audit approach. These are:

- The results of previous audit procedures, and
- The nature and timing of the audit procedures.

The results of previous audit procedures will be explained in each of the various steps below. As highlighted in this dissertation, the Internet is inherently considered to be a high risk area. The timing of the audit procedures for EC payment security is therefore of such a nature that the audit needs to be performed as soon as an organisation starts trading over the internet and planned procedures and controls should be evaluated prior to the commencement of such trading. Thereafter, due to the high risk nature of EC payment security, the audit procedures should be performed on a cyclical basis as for all other high risk areas, or whenever major changes occur in the environment. The factors influencing the timing of the EC payment security audit are therefore summarised as:

- Results of previous audit procedures;
- Changes in the environment, and
- The nature of risks in the environment.

The audit approach further incorporates the nature, timing and extent of audit procedures to be applied during an audit. This will be addressed as part of the approach defined in Section 6.4 below. The nature of a planned audit procedure refers to the method used by the particular procedure to gather the evidence. Some methods of gathering evidence (e.g. observation, vouching, inquiry) are considered to gather evidence of greater reliability than others (Abrema, 2002). Detailed audit considerations have been included in Appendix A of this dissertation. These detailed considerations have been excluded in this chapter because they do not form part of the formulation of the audit approach. They are however considered to be important for the IS auditor, because they provide detail that would assist the IS auditor to ensure all risks are considered.

These detailed considerations do not always apply to all environments due to the fact that all EC environments do not necessarily contain the same technologies e.g., firewalls, routers, intrusion detection systems .

6.4 CONSIDERATIONS ON AUDIT PROCEDURES FOR AN EC PAYMENT SECURITY AUDIT

6.4.1 STEP 1 SCOPE AND UNDERSTAND THE ENVIRONMENT - BACKGROUND INFORMATION GATHERING

The background information related to EC payment security was covered in Chapter 3 of this dissertation. The following factors are considered to affect the scope of an information systems audit in the EC payment security environment (EDPAA, 1983):

- Time – the amount of time allocated to complete the audit;
- Talent/skills – the type of audit skills available to conduct the audit as well as the support available from other non-audit departments;
- The tools and techniques available to the audit staff to conduct the audit. An EC payment security environment may be very technical and the technology used in the process is usually the latest available. For example, the auditor may have to use tools such as network scanning tools to determine vulnerabilities that can't be determined in another way;
- The results of previous audit procedures – this will be discussed in more detail below.

6.4.1.1 The Results of Previous Audit Procedures

As a first step, the IS auditor should review the permanent file related to the EC payment security environment. This will provide background that will serve as a starting point to the audit. Other factors that need to be determined include determining the changes to the environment since the last audit. If the IS auditor is completely unfamiliar with the environment, background information should be gathered through techniques such as interviews with the auditee and reviews of published and available material from the auditee or vendors used by the auditee. For the vendor related documentation, the Internet may also be used as a source because many vendors publish white papers about their products on their web sites. Other sources of information are the product manuals provided by vendors with their hardware or software and published books. Background information to EC payment security was provided in Chapter 3.

As further assistance to the IS auditor, more detailed aspects related to information gathering have been highlighted in Section 1 of the Appendix A of this dissertation. The questions contained in the Appendix will serve as a guideline for the information gathering process in an EC payment security audit. For the purposes of this dissertation, the information gathering is further divided into general IT information, EC specific information, and legal considerations.

6.4.1.1.1 General IT Environment Information Gathering

The information gathering guidelines related to the general IT environment, as highlighted in Appendix A of this dissertation are used to obtain a general understanding of the IT environment in an organisation. However, EC-specific information is also required so that the auditor will understand how EC-related technology fits into the overall environment.

6.4.1.1.2 EC Specific Information Gathering Considerations

The information-gathering guidelines and considerations specifically related to the EC environment have been highlighted in Chapter 3. Further checklists and questions to assist the IS auditor in this information gathering process have been included in Appendix A of this dissertation.

6.4.1.1.3 Legal Considerations

A non-IS audit is usually conducted on the legal compliance of an entity trading on the Internet. The IS auditor should however ensure that legal considerations regarding the payment have been included in such a review. The following should be considered:

- Describe the entity's policies and procedures to provide reasonable assurance that it complies with local and international legal requirements;
- Where required by such requirements, describe how appropriate disclosures are provided to the customer.

Data protection is only one of the major issues that need to be addressed. As indicated in this dissertation, consumers and businesses are apprehensive about misuse of information held on the Internet. For example, the UK's statutory approach

is embodied in the Data Protection Act 1984, as updated by the Data Protection Act 1998, which brings the 1995 Electronic Commerce Data Protection Directive into UK legislation. It will be necessary for the proposed business frameworks and data protections legislation to be kept under review so that effective protection is evident when engaging in electronic commerce (ICAS, 1998).

The IS auditor should determine whether the following legal factors have been considered:

- **Copyright**: if links are provided on a website, do sites linked to have to agree? Do links constitute a breach of copyright? In principle viewing a site involves copying its content to a cache on viewer's computer/server. Is there an implied license by web site owners to view? Does this extend to downloading and printing?
- **Security**: how far do professional service suppliers, for example accountants or lawyers, have to ensure a web site is secure, hacker free etc. If not, is this a breach of clients' rights to confidentiality?
- Are there any issues of **data protection**? Any business storing personal data (including emails) may need to register and guard against cross border data flows to non-data protection regime countries, for example the United States.
- How is **payment** to be made? In general, each digital cash scheme has a different legal set up, usually not apparent to a participating supplier or purchaser.

6.4.1.1.4 Special Rules

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 a client's electronic systems: increasingly there is exposure to electronic vandals, criminals and other threats. For example (*ICAS*, 1998), 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.

The IS auditor should understand the client's business philosophy, strategy and business processes. Central to this is a detailed understanding of the impact of

technology and the client's underlying systems. Questions then arise about the status of a computer server, the computer itself, the positioning of the telecommunications equipment and the usual agency problems. For example, do aspects such as double taxation agreements apply?

At the end of this phase the IS auditor should have sufficient information and understanding to continue to the next step of the audit approach. However, the IS auditor may require more information in subsequent steps and may therefore perform additional information gathering activities to be able to complete the audit of EC payment security.

6.4.2 STEP 2 - RISK ANALYSIS CONSIDERATIONS

The risk analysis considerations in an EC environment have been identified and described in detail in Chapter 4 of this dissertation. The risks present in the EC payment security environment may be identified using the information gathered in the background information gathering phase of the audit, brainstorming, past experience, and lists of risks common in information systems. The information gathered in the first step of the audit approach plays a significant role in the risk identification and analysis process. As part of this risk identification process, the results of previous audit procedures also need to be considered. This aspect will be addressed in Section 6.3.2.1 below. Another factor to be considered is the magnitude of the risk. To devote significant audit resources to low risk areas would be inappropriate as it may result in higher risks not being addressed. The magnitude of risk may be determined through either:

- The evaluation of historical information;
- Risk ranking by the audit team in conjunction with management;
- Through applying formulas (i.e., the likelihood of an event times the loss associated with the occurrence of an event, expressed as a monetary value), or
- A combination of the above methods.

A last step in the risk analysis process is to prioritise the risks. This process involves the determination of the importance of the risk to the audit process. The calculation method or the risk ranking method mentioned above will usually result in risk being rated as High, Medium, or Low. The main focus of the audit will be to ensure that at

least high risk areas are addressed. If audit time allows, medium and low risk areas should also then be considered.

6.4.2.1 Results of Previous Audit Procedures

The results of previous audit procedures will also affect the audit approach. In an audit of electronic commerce payment security, any results from audits in the following areas will influence the EC payment security audit approach:

- Networks, including firewall and router administration;
- Corporate information security office (CISO) including security policies and procedures and security administration;
- Business Continuity Planning (BCP);
- Change management;
- Physical security and environmental controls;
- Data center operations review, including backup;
- Operating Systems and web server review (e.g., Windows NT, Unix, OS/390, Windows 2000, etc);
- Application audits for EC payments application systems.

Where reliance is placed on areas subjected to previous audit procedures by either the internal or external audit departments of an organisation, the purpose is to ensure that the considerations related to EC payment security have been included in such a previous audit. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the timing, nature, and extent of the current EC payment security audit procedures and also assess management actions taken since the last audit/ review.

6.4.2.2 Risk Considerations for EC Payment Security

As highlighted in Chapter 4 of this dissertation, the risks in an EC payment security environment focus on the following six elements:

1. Unauthorised access;
2. Data alteration/Integrity;
3. Breach of confidentiality/Privacy;

4. Denial of Service/Availability;
5. Repudiation;
6. Authentication.

These elements are translated into the following risks:

1. Lack of access control and authorisation may result in unauthorised changes to data or inaccurate data;
2. Lack of integrity may result in inaccurate processing of transactions;
3. Lack of privacy or confidentiality may result in fraudulent transactions or interception of information during transmission;
4. Lack of intrusion detection and monitoring procedures may result in system availability being compromised and possible subsequent loss of revenue and negative publicity;
5. Lack of authentication, integrity, and confidentiality may result in repudiation of transactions;
6. Lack of adequate authentication procedures may result in unauthorised access and unauthorised changes to data.

These risks represent the focus of the audit approach and due to the nature of EC payment security, these are considered "High Risk". This is due to the fact that if the risks are not properly controlled, the exploitation of weaknesses could have a significant impact on the overall control environment and on an organisation's business activities. The control considerations section (see 6.4.3 below) will identify controls to mitigate these risks.

6.4.3 STEP 3 - CONTROL CONSIDERATIONS

As stated in the risk section (6.3.2.1) above, the results from previous audit procedures should be considered during the current audit. The extent to which controls have been addressed in the various audits, as mentioned in Section 6.3.2.1 above, will determine if any additional focus is required in those areas when conducting an EC payment security audit.

Control considerations in an EC payment security environment were highlighted in Chapter 5 of this dissertation. The control considerations and procedures that need to be taken into account as part of the audit approach will be highlighted in this

section. Table 1 below associates the risks mentioned above with the control procedures required to be performed by the IS auditor in the EC payment security audit. (Numbers 1 to 6 in the top row of the table refer to the risks mentioned in Section 6.3.2.2 and the Reference refers to the control procedures section that follows the table). Detailed audit considerations and procedures have been included in Appendix A of this dissertation.

Table 6.1 Risk/Control Matrix

Controls\Risks	**1**	**2**	**3**	**4**	**5**	**6**	**Reference**
General Controls*							
Security policies, corporate information security, and security administration	X	X	X	X	X	X	6.4.3.1.1
Physical and environmental security	X	X	X	X	X	X	6.4.3.1.2
Operating system and web server vulnerabilities/controls	X	X	X	X	X	X	4.3.1.3
Change management	X	X	X	X	X	X	6.4.3.1.4
Business continuity planning	X	X	X	X	X	X	6.4.3.1.5
Organisational structure	X	X	X	X	X	X	6.4.3.1.6
Computer operations and backup	X	X	X	X	X	X	6.4.3.1.7
Legal compliance	X	X	X	X	X	X	6.4.3.1.8
Event Journalling	X	X	X	X	X	X	6.4.3.1.9
Controls\Risks	**1**	**2**	**3**	**4**	**5**	**6**	**Reference**
Technical EC controls							
Encryption, privacy, and secure protocols*1		X	X		X	X	6.4.3.2.2
Digital certificates/signatures*1	X	X			X	X	6.4.3.2.3
Firewall and router considerations	X			X			6.4.3.2.1
Public Key Infrastructure (PKI)		X	X	X	X	X	6.4.3.2.3
Intrusion Detection Systems	X			X			6.4.3.2.4
Virtual Private Networks (VPN)*2	X		X	X			6.4.3.2.5

*1 - Secure payment protocols and PKI use encryption and digital certificates

*2 - A VPN uses firewall technology and encryption

* - General controls apply across all sections. I If general controls are not in place, it doesn't matter what specialised controls are implemented as a lack of general control may potentially override any specific controls.

6.4.3.1 The Nature of the Audit Procedures

The nature of a planned audit procedure refers to the method used by the particular procedure to gather the evidence. Some methods of gathering evidence (e.g. observation, vouching, inquiry) are considered to gather evidence of greater reliability than others (Abrema, 2002).

The nature of the audit procedures in an EC payment security environment assists the IS auditor in determining the tests to be performed. The nature and extent of the audit procedures is further dependent on the information obtained and the risks, and due to the complexity of the technology in the EC payment security environment, the considerations covering the nature and extent of the auditing procedures have been included in Appendix A. The considerations highlighted in Appendix A apply to all the control areas mentioned under Section 6.4.3. Due to the level of detail required to provide detailed listings related to the nature and extent of the procedures, these considerations have been shown separately in Appendix A.

6.4.3.2 General Control Considerations

General controls refer to those controls that are used in the system development and computer processing activities. The general controls have been indicated in the above-mentioned table as applicable across all the risk factors. The reason is that weaknesses in the general controls area may have a significant impact on the risks related to EC payment security. This impact can potentially render any specific controls ineffective (SAICA, 1998); (AARF, 2000). The purpose of this section is not to provide a complete audit program to cover all the technologies used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. Where reliance is placed on areas subjected to previous audit procedures by either the internal or external audit departments of an organisation, the purpose is to ensure that the considerations mentioned below and in Appendix A have been included in such previous audit procedures. This should be achieved through a review of the audit programs for the sections evaluated, a review of the audit reports, a review of the audit planning memorandums detailing the audit objectives, and/or discussions with the auditors responsible for the reviews.

The aspects mentioned below and in Appendix A will also apply to the audit of a Certification Authority (CA). Because the CA plays such a significant role in the digital certification process, the IS auditor needs to consider all the aspects related to the CA. Where specific procedures only apply to the CA, this is indicated in the considerations. The main aspects related to CAs and digital certificates and encryption will be discussed in more detail in the PKI section (6.4.3.2.3) below.

6.4.3.2.1 Security Policy, Corporate Information Security (CIS) and Security Administration

A security policy, Corporate Information Security Office (CISO), or security administration review would normally be performed as a separate audit(s). The IS auditor should ensure that aspects related to EC has been included in such a previous audit. The IS auditor should therefore ensure that aspects mentioned in this section and the detailed considerations in Section 2.1 of Appendix A have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

A security policy needs to lay out, in writing, the security processes of an organisation and outlines the aspects of who, what, when, how, and why of ongoing actions and procedures. It should be a detailed document that identifies risks, defines steps taken to reduce them to acceptable levels, and outlines the tasks and job-descriptions of those directly involved in the enforcement of security in an organisation.

The auditor needs to determine whether formal security policies and security standards documents are tailored specifically for each networking environment. The auditor also needs to determine whether periodic assessments of systems, policies, and procedures are performed to provide for effective augmentation of existing security programs, and the implementation of new security measures and countermeasures. The detailed audit considerations related to the security policy, security organisation, and security administration, have been included in Appendix A.

Security administration also includes monitoring activities related to intrusion detection, and this is covered under Section 6.4.3.2.4 below.

6.4.3.2.2 Physical and Environmental Security

An effective network defense is not complete if someone can physically gain access to equipment or to private networks. A physical and environmental security review would normally be performed as a separate audit. The controls around physical and environmental security have been highlighted in Chapter 5 of this dissertation. The purpose of addressing this area in an EC payment security audit is not to provide a

complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in Section 2.2 of Appendix A have been included in previous audit procedures. Where weaknesses were identified during a physical or environmental security audit, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

6.4.3.2.3 Operating System and Web Server Considerations

An operating system or Web server review would normally be performed as a separate audit. The controls around operating systems and Web servers have been highlighted in Chapter 5 of this dissertation. The purpose of addressing this area in an EC payment security audit is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review. The IS auditor should review procedures to ensure that the considerations as highlighted in Section 2.3 of Appendix A (that should be performed by the appropriate auditee personnel), have been included in an operating system review:

One component often overlooked in all the various security models, methods, and protocols, is the end user's computer. No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end user's computer. That computer has stored all the digital certificates, most of the consumers' personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers, which store information in some very basic forms, even plain text. This use means the consumers' financial and banking data is only as secure as that computer. To further complicate matters, there are many laptop computers used in homes and in businesses. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data. Controls that will minimise this risk (i.e., physical security, access controls and policies) were addressed in Sections 6.4.3.1.1 and 6.4.3.1.2 above.

6.4.3.2.4 Change Management

A change management review would normally be performed as a separate audit. The controls related to change management have been highlighted in Chapter 5 of this dissertation. The purpose of addressing this area in an EC payment security audit is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in the change management section (Section 2.4) of Appendix A, have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

6.4.3.2.5 Business Continuity Planning (BCP)

Audit Considerations

A BCP review would normally be performed as a separate audit. The controls related to BCP have been highlighted in Chapter 5 of this dissertation. The purpose of addressing this area in an EC payment security audit is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in Section 2.5 of Appendix A have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

Note: Encryption key compromise is considered one type of "disaster." CA termination is included under business continuity planning, because in the event the CA terminates, policies and procedures should be in place to ensure the continuity of service to customers.

6.4.3.2.6 Organisational Structure

Audit Considerations

The auditor should consider performing procedures to determine whether the personnel security requirements for job definition, hiring, and training, as stated in the

applicable security-related documentation, are being achieved. Detailed considerations have been highlighted in Section 2.6 of Appendix A.

The audit procedures related to intrusion detection (i.e., the monitoring responsibility of staff) is covered in more detail in Section 6.4.3.2.4 below.

6.4.3.2.7 Computer Operations and Backup

Audit Considerations

A computer operations and backup review would normally be performed as a separate audit. The controls related to computer operations and backup have been highlighted in Chapter 5. The purpose of addressing this area in an EC payment security audit is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in this section and in Section 2.7 of Appendix A have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

6.4.3.2.8 Legal Compliance

Audit Considerations

As stated in Section 6.3.1.1.3 above, a non-IS audit is usually conducted on the legal compliance of an entity trading on the Internet. The IS auditor should however ensure that legal considerations regarding the payment have been included in such a review. Apart from the procedures in the relevant section mentioned above, the auditor should consider performing the following procedures to determine whether the requirements for compliance with legal requirements, as stated in the applicable security-related documentation, are being achieved:

- Review the company policy and determine whether it specifies procedures related to the copying of software;
- Review the company guidelines for the retention, storage, handling and disposal of company records and ensures it adheres to legal requirements;

- Review the company policy and ensure that it includes procedures for data protection;
- Interview relevant personnel, for example from the legal department.

6.4.3.2.9 Event Journal

Audit Considerations

The auditor should consider performing the following procedures to determine whether the requirements for event logging and archiving, as stated in the applicable security-related documentation, are being achieved:

Review event journal and assessment reports and ensure the following are specified, and ensure they are related to the logs:

- Specific events to be recorded in the event journal;
- Specific items to be captured and recorded for each event;
- Length of time for retention of the archived event journal;
- Events that are recorded automatically/electronically and/or manually;
- Confidentiality and integrity of the event journal during its generation;
- Confidentiality and integrity of the event journal during storage and transmission;
- Periodic archival of the event journal;
- Archival of the event journal at a secure off-site location for a pre-determined period;
- Periodic review and reconciliation of the event journal;
- Interview personnel responsible for monitoring logs and reports;
- Compare event journal contents and procedures to best practices as defined in ISO 15782-1.

6.4.3.3 EC Specific Technical Security Control Considerations

6.4.3.3.1 Firewall and Router Considerations

A router and/or firewall audit would normally be performed as a separate audit. The controls related to firewalls and routers have been highlighted in Chapter 5. The purpose of addressing this area in an EC payment security audit is not to provide a complete audit program to cover all the aspects used for control purposes, but rather

to provide considerations that need to be taken into account by the IS auditor. The IS auditor should ensure that aspects mentioned in this section and in Section 2.8 of Appendix A, have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact on the EC payment security audit and assess management actions taken since the last audit/ review.

The role of the IS auditor in this respect would therefore be to ensure that the firewall/ router audit covered a review of the controls and procedures as detailed in Appendix A.

6.4.3.3.2 Encryption, Privacy, and Secure Protocols

One of the objectives of encryption and secure protocols is to ensure information protection, i.e., ensure that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business. The controls related to encryption and secure protocols have been highlighted in Chapter 5. As highlighted there, encryption is regarded as a very important control for EC payment security. Primary considerations that should be evaluated by the IS auditor have been included in Section 2.9 of Appendix A.

The aspects related to encryption keys and digital certificates are addressed in the PKI section below.

6.4.3.3.3 Public Key Infrastructure (PKI) Considerations

Note that aspects mentioned in the sections above may also be used to evaluate and assess the adequacy of control over the same activities of the Certification Authority (CA) responsible for the digital certification process. These areas include the following:

- Security Policy, CIS and Security Administration should also address the Certificate Practice Statement (CPS) content;
- Physical and environmental security;
- Operating system and web server considerations;
- Change Management;
- Business Continuity Planning;
- Organisational Structure;

- Computer Operations and backup;
- Legal compliance.

The aspects mentioned under the PKI section below and detailed in Appendix A, will also apply if the organisation being audited functions as a CA and issues and manages its own certificates. Where the organisation uses a public CA (e.g., Verisign), these audit steps mentioned below will be covered in a review of the public CA. Where special procedures apply, appropriate reference is made in each section to the CA, RA or CPS. As indicated in the encryption section above, the aspects related to encryption and secure protocols are also discussed below. The aspects mentioned for key management activities below can also be applied to any encryption key management process.

The auditor should evaluate reports (internal or external) related to the CA organisation and evaluate the impact of weaknesses identified in these reports on the EC payment security audit. The auditor should determine whether compensating controls are in place to address such weaknesses.

For the purposes of detailed audit procedures and considerations, PKI is divided into the following areas (the detail audit procedures related to each of these areas is provided in Section 2.10 of Appendix A):

Key Management Life Cycle Controls:

- Key Generation
- Key Storage, Backup and Recovery
- Key Distribution
- Key Escrow
- Key Usage
- Key Destruction
- Key Archival

Device Life Cycle Management:

- Device Shipment
- Device Receipt

- Device Pre-Use Storage
- Device Installation and de-installation
- Device Usage
- Device Service and Repair

Certificate Life Cycle Controls:

- Initial Certificate Registration
- Subsequent Certificate Renewal
- Subsequent Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Revocation List (CRL) Processing

6.4.3.3.4 Intrusion Detection

Audit Considerations

The controls related to intrusion detection have been highlighted in Chapter 5. The purpose of addressing this area in an EC payment security audit is to ensure that intrusion detection aspects were covered in the appropriate review. Appendix A (Section 2.11) contains detailed considerations for the IS auditor. Some of these considerations were covered in an operating system/server vulnerability or a firewall review. Where applicable, this is indicated for each consideration mentioned in Appendix A. The IS auditor needs to ensure that intrusion detection aspects were covered in the appropriate review. This is normally done by evaluating the results of such review and evaluating the impact of negative findings on the risks in the intrusion detection area.

6.4.3.3.5 Virtual Private Networks (VPN) Considerations

A well-designed VPN should incorporate security, reliability, scalability, network management, and policy management. A VPN should use several methods for keeping a connection and the data secure:

- **Firewalls** – firewalls may restrict the number of open ports and the packets and protocols allowed through. Firewalls were discussed in Section 6.4.3.2.1 above.
- **Encryption** – encryption was discussed in detail in Section 6.4.3.2.2 above.
- **IPSec** – IPSec is a secure protocol that provides enhanced security features such as better encryption algorithms and comprehensive authentication and integrity checking. Other examples of secure protocols are PPTP and L2TP. Secure protocols were addressed in Chapter 5 and in Section 6.4.3.2.2 above.
- **Tunneling** – VPNs rely on tunneling to create a private network that reaches across the Internet. Tunneling is the process of placing an entire packet within another packet and sending it over the network. The protocol of the outer packet is understood by the network and by the points where the packet enters and exits the network.

6.5 CONCLUSION

The approach to an audit highlights the steps to be followed when the auditor is involved in an audit. The purpose of this dissertation is to develop such an audit approach for the IS auditor for an EC payment security audit. As indicated in this chapter, the audit approaches followed by the major public accounting firms, as well as numerous other audit organizations and departments, are risk-based and involve the following steps:

- Scope and understand the environment;
- identify the risks, and
- identify the controls to address these risks.

This chapter also documents other aspects that have an influence on the audit approach, such as the results of previous audit procedures and the timing of the audit procedures.

As highlighted in this chapter, the audit of EC payment security involves a very wide spectrum of technologies and includes many audit areas. The results of previous audit procedures therefore play an important role in reducing the audit areas and enabling the IS auditor to focus the audit efforts. This chapter provided an easy-to to-use table (in Section 6.3.3) to link the risks and the controls. This table serves as a

guide to the IS auditor to identify the areas of an audit in the EC payment security environment.

Detailed audit considerations have also been provided in Appendix A to enable the IS auditor to follow a structured approach to gather background information and to have adequate audit considerations available that could be used to develop an audit program and audit tests in an EC payment security audit.

6.6 FORMULATING THE AUDIT APPROACH FOR THE IS AUDITOR: AN OVERVIEW

This dissertation showed that there are various types of auditors and highlighted the roles and responsibilities of the IS auditor. In Chapter 2 it was highlighted that the role of the IS auditor involves the evaluation of the controls in the IS environment as part of their responsibility to management of the organisation and other interested parties. This role also includes understanding the IT environment (including computer jargon and technologies), identifying weaknesses and risks, and adding assurances to management and other interested parties. The role of the IS auditor is defined either in the capacity of an external or an internal auditor.

It was also shown that auditors must ensure that appropriate audit resources are applied to those issues that concern executive management. They must bring new information, positive or negative, to management's attention in such a way that management will understand its importance and act appropriately.

Electronic commerce is a broad and varied field prone to technical complexity. Understanding and assessing controls in this environment force IS auditors to continuously update their skills and to provide management of an organisation with assurance on the control environment for this new technology. It was shown that the IS auditors need to adhere to the standards of the professional organisations that they belong to. These standards also require the IS auditor to keep their skills and knowledge up to date with changes in the IT environment. It was also highlighted that there have been developments in the audit area that provide guidance to the IS auditor in an EC environment.

An audit approach outlines the manner or method of performing an audit and includes certain steps that need to be taken. This dissertation highlighted the steps to be followed by an IS auditor when an audit of electronic commerce payment security is conducted. The steps have been defined as follows:

- Scope and understand the environment – background information gathering
- Identify risks in the EC payment security environment
- Identify controls to minimise the risks.

These three steps were detailed in this dissertation as follows:

Chapter 3 identified the importance of electronic commerce and highlighted the fact that electronic commerce is a very new technology, which will be important to future business and therefore to the IS auditors. There are many aspects to the e-commerce technology that must be understood by the IS auditor. Especially in the areas of electronic payments, there are many vulnerabilities which need to be addressed. IS Auditors must be aware of all the vulnerabilities as well as the controls available to address these risks.

Chapter 4 identified the unique risks in the EC payment environment. It was shown that these risks stem from the fact that the Internet has been designed to be "open", which increases the likelihood of manipulation. The need for security and control in this environment has also been highlighted. It was established that the IS auditor needs to be aware of the inherent risks in an EC payment security environment to enable him/her to identify such risks when an area involved in EC payments is being evaluated/reviewed. The IS auditor plays an important role in the risk management process through the risk identification process, and armed with knowledge of the risks, the IS auditor is able to identify and evaluate controls required to minimize or manage the overall risk.

Chapter 5 identified the elements of a secure business environment and also indicated that each is a necessary component for a complete solution. The technologies available to control each of the elements were also identified.

It was also highlighted in Chapter 5 that the audit of the security of EC payments is not a single task or subject but involves many different technologies that need to be

taken into account and many of the technologies, if correctly used will aid in securing EC payments. The role of the auditor is to understand the available technologies, assess the risks of implementing the technologies and to identify the controls required to ensure that the technologies will provide the assurance required. When the IS auditor understands the available technologies and the controls they provide, this enables the development of an audit approach. The technologies and risks addressed by the implementation of the technologies are highlighted in Table 6.2 below.

The audit approach was defined in Chapter 6 and involves the execution of the three steps mentioned above and addressed in the previous chapters. The execution of the steps also involves the consideration of previous audit procedures and the timing of the audit procedures.

The audit approach identified in this dissertation provides the IS auditor with sufficient detail to approach an EC payment security audit by firstly obtaining background information. (This dissertation includes detailed audit procedures to obtain background information.)
The audit approach secondly identifies the risks in the environment. Detail regarding the risks is provided and is also part of the audit approach. The risks are also listed in Table 6.2 below. The auditor may therefore use the risks identified as the focus of the audit procedures.
Thirdly, this dissertation identified controls to address the risks. Detailed information regarding controls and technologies available were also provided. The control and technology areas are also listed in Table 6.2 below. The audit approach identified the audit procedures that could be used by the IS auditor to evaluate the controls. Appendix A provides detailed considerations to assist the auditor in identifying and evaluating controls.

Table 6.2 below represents a summary of the most important conclusions of this dissertation. It depicts the relationship between the risks and controls in the EC payment security environment. The risks identified as numbers 1 through 6 in the table have been described in Chapter 4 and have been included below the table for ease of reference. Each of the crosses ("X") in the columns of the table indicates that the control will address the risks identified. Note that each control cannot be interpreted in isolation, i.e., to evaluate the control in an EC environment, all the controls need to be considered. For example, if the physical and environmental

security controls adequately address the risks, this will not provide assurance over the complete EC environment. All other applicable controls also need to be evaluated.

Table 6.2 Risk/Control Matrix for EC Payment Security

Controls\Risks	**1**	**2**	**3**	**4**	**5**	**6**
General Controls*						
Security policies, corporate information security, and security administration	X	X	X	X	X	X
Physical and environmental security	X	X	X	X	X	X
Operating system and web server vulnerabilities/controls	X	X	X	X	X	X
Change management	X	X	X	X	X	X
Business Continuity Planning	X	X	X	X	X	X
Organisational structure	X	X	X	X	X	X
Computer operations and backup	X	X	X	X	X	X
Legal compliance	X	X	X	X	X	X
Event Journaling	X	X	X	X	X	X
Technical EC Controls						
Encryption, privacy, and secure protocols*1		X	X		X	X
Digital certificates/signatures*1	X	X			X	X
Firewall and router considerations	X			X		
Public Key Infrastructure (PKI)		X	X	X	X	X
Instrusion Detection Systems	X			X		
Virtual Private Networks (VPN)*2	X		X	X		

*1 - Secure payment protocols and PKI use encryption and digital certificates

*2 - A VPN uses firewall technology and encryption

* - General Controls apply across all sections due to the fact that if general controls are not in place, it doesn't matter what specialised controls are implemented as a lack of general control may potentially override any specific controls.

1. Lack of access control and authorisation may result in unauthorised changes to data or inaccurate data.
2. Lack of integrity may result in inaccurate processing of transactions.
3. Lack of privacy or confidentiality may result in fraudulent transactions or interception of information during transmission.
4. Lack of intrusion detection and monitoring procedures may result in system availability being compromised and possible subsequent loss of revenue and negative publicity.
5. Lack of authentication, integrity, and confidentiality may result in repudiation of transactions.
6. Lack of adequate authentication procedures may result in unauthorised access and unauthorised changes to data.

6.7 THE ROLE OF THE IS AUDITOR: FINAL OBSERVATIONS

This dissertation provides the following framework for an EC payment security audit approach for the IS auditor:

- Gather background information related to EC payment security;
- Highlight the risks in this environment;
- Identify possible controls that will minimise the risks;
- As part of the audit approach, this dissertation also highlighted the considerations that may be used by the IS auditor when an audit in the EC payment security area is being performed. These considerations are based on the underlying technologies, general controls, and EC-specific issues e.g., PKI, digital certificates, etc.

This dissertation therefore provided the IS auditor with a complete approach to an EC payment security audit and included audit considerations. The remaining steps and procedures required by an IS auditor is to perform audit tests, evaluate the results, and report on any findings.

EC is a growing business option and due to the "openness" of the underlying technologies used for EC, introduces new risks and new technologies that require sophisticated and sometimes very technical controls to be implemented. The IS auditors need to be technically competent to understand the impact of new technologies on the control environment and at the same time IS auditors need to be able to communicate the audit results to non-technical management.

The audit approach to an EC payment security audit does not differ significantly from an audit approach for other IS audits. The IS auditor still needs to perform the steps highlighted in the framework above.

The differences therefore arise due to the changing EC technological environment. This requires the IS auditor to usually spend more time in understanding the business processes and especially the underlying technologies. Many of the aspects related to non-EC specific audits still apply, e.g., a general controls assessment. In an EC audit, the IS auditor will have to rely on the results of previous audit procedures to avoid getting "bogged down" in one audit (EC payments security). This means that the IS auditor is attempting to evaluate all technologies used in EC payment security simultaneously. As an example, consider that the EC payment security environment involves networks (including routers and firewalls) and possible web servers operating in a general control environment (including data centre operations, physical security, change management, contingency, and many others).

The IS auditor should therefore plan an EC payment security audit very carefully and consider breaking down the audit into manageable units and sub-units where s/he reliance may be placed on previous audit procedures.

The IS auditors have an ongoing responsibility to ensure that they keep up to date with changes in technologies especially changes related to EC and in this particular research, EC payment security. This is due to the fact that EC is constantly redefining the current business processes, and technologies are improving exponentially. The IS auditors should assess their own procedures used to update themselves on developments in EC and related technologies. This should be done so that the IS auditor will be prepared to advise management on the impact of new technologies on the internal control environment in an organisation. The IS auditor needs to play a proactive role in assessing risks and controls. As part of this process the IS auditors need to identify processes to evaluate their own skills against the changing requirements brought about by developments in EC, and supplement shortcomings with training (internal, external, or self-training). The IS auditor's skills need to be more refined and more innovative because EC technologies take IS auditors to areas that have not been assessed before and where limited information is available. This dissertation provides and IS auditor with the information required to understand the EC payment security environment, and by following the audit approach defined here, the IS auditor is able to speed up the audit process and be prepared to develop an audit program with audit tests. The audit considerations defined in this dissertation will further assist the IS auditor in the audit program preparation.

In an EC payment security environment the IS auditor needs to rely on many new software products to identify weaknesses in a system e.g., port scanners to identify activated ports for network related traffic. The results of such automated procedures should still be interpreted by the IS auditor. Without these tools, the IS auditor may not be able to fully assess the risks in the environment. The IS auditor should therefore also be aware of new technologies that may be used to assist in the performance of the audit tests. IS auditors should develop a process to update themselves on changes in these types of software and audit tools.

The IS auditors should understand that they can not be experts in all the different technologies related to EC payment security. They should arm themselves with the knowledge to understand the risks involved with new technologies and they should

have a sufficiently in depth background exposure to technology to understand the controls required to address the risks.

This study also identified the following areas where further research regarding the role of the IS auditor in an EC environment is required:

- The effects of automated audit and management/monitoring tools on the audit testing phase of an EC audit. Many tools have been developed to monitor activities (e.g., security incidents, system performance, intrusion detection, etc.) in an EC environment. The introduction of such tools enables management to identify possible problems and to react in a timely manner. Many of these tools, as well as other specialised audit tools, are also valuable to the IS auditor and may be used to effectively manage the audit effort. The IS auditor should develop procedures to evaluate such tools for audit use to render a more value-added service to management.
- How auditors should prepare themselves to remain up to date with the changes in EC technology and the effects on the audit procedures. One of the most difficult issue for an IS auditor is to remain up to date with technology i.e., to understand new technology and be able to assess its impact on the control environment. There are various ways to obtain knowledge of new technologies and the risks e.g., self study, membership of professional organisations and mailing groups, external courses, seminars or formalised study methods. The emphasis is on the audit department to find the right balance of methods to ensure they perform a value added service for the organisation's management.
- How auditors should meet the expectations of management with relation to the automation of business processes (through complex technologies) especially with the subsequent loss of the audit trail. Auditors need to find new ways of reviewing control documentation, and tools such as Computer Assisted Auditing Techniques (CAATs) become essential to the auditor's toolbox. The secret is to design these CAATs to serve the auditor and to ensure that management implements the controls function properly.

APPENDIX A

THE NATURE OF AUDIT PROCEDURES IN AN EC PAYMENT SECURITY AUDIT

INDEX

1 Introduction – Purpose of this Appendix

The audit considerations mentioned in this Appendix are related to an audit in an EC payment security environment and assist the IS auditor in determining the audit procedures and tests to be performed. The nature and extent of the audit procedures are further dependent on the information obtained and the risks in the environment. Due to the complexity of the technology in the EC payment security environment, the considerations covering the nature and extent of the auditing procedures have been included separately from Chapter 6 in this Appendix. This is also due to the level of detail required to provide detailed consideration listings related to the nature and extent of the procedures.

This Appendix shows the audit considerations related to the steps in the audit approach as highlighted in Chapter 6 of this dissertation. Firstly, the considerations related to Background information gathering is provided in Section 2, followed by the considerations related to the controls in Section 3. In Chapter 6, the reference to the detailed considerations was provided with each control area, where applicable. Chapter 6 and this Appendix should therefore be used together to obtain the maximum benefit from the information provided.

2 BACKGROUND INFORMATION GATHERING AUDIT CONSIDERATIONS

2.1 GENERAL IT INFORMATION GATHERING CONSIDERATIONS

The following tables contain guidelines for information that should be gathered by the IS auditor to obtain an understanding of the EC environment in an organisation.

Table A1 IT Information to be Obtained

IT Information			
Outsourced functions (Consider IT operations, systems development, web development, web hosting, ASP, IT Internal Audit):			
Hardware platforms (Consider central IT, localised IT, e Commerce, m Commerce):			
e.g. AS/400, UNIX, OS/390			
External links e.g. routers, firewalls (please detail): Operating systems and other system software (please detail): No. of WANs [ ] No. of LANs [ ]			
Application software that supports key EC business processes (please detail):			
Name	Supplier *(or in house)*	Key business process	Date developed/implemented

Table A2 Hardware Platform Configuration Information to be Obtained

Hardware Platform Configuration (make and model)	Number	Number of Terminals
Mainframe		
UNIX Environment		
Windows NT/W2K Environment		
Other Platforms		
• PC(s)		

Table A3 IT Installation Information to be Collected

IT Installation		
Operating Systems in use	**Version**	
IBM (e.g., OS/390)		
UNIX (e.g., HP-UX, Solaris, AIX)		
Windows NT/W2K		
PC		
Other		
Programming Languages or 4GLs (Powerbuilder, Developer 2000 etc.)	**Version**	**Running on**
Access control software (Safeguard, Intel LanDesk Protect etc)		
Database management system (e.g., DB2, Oracle, Sybase, Adabas, RACF, ACF2)		
Network Scanning and Intrusion Detection tools used (e.g., ITA, Axent/ESM, Netprowler)		
Others		
Disk or tape management systems		
Document Management		
Report Generators		
Audit Software		

Table A4 EC Application System Information

EC Application systems software	Date installed	Computer used	Comments (e.g. in-house or packaged software, EDI, e-commerce, batch,on-line)	WP Ref
Accounting				
Other applications				

Information on significant EC Applications used to support to EC activities

Consider the specific setup of application(s) that are considered significant.

Table A5 General EC Application Information to be Obtained

Name of Application (e.g.. package name):	
Designated Owner:	
Description of the Application:	

Major Modules / Functions of the Application:

....

Table A6 EC Specific Application System Information to be Obtained

• Package or In-house developed:	• Package/software maintenance supplier:
• Installation Date:	• Version of software:
• Source code owned or available: • Program Language:	• Extent of modifications:
• Number of Users:	• User satisfaction ranking (good-5 low-1)
• Is the system documented:	• Interfaces:

Is the system considered to be stable? (Please comment.)

Was there sufficient training on the systems?

2.2 EC SPECIFIC INFORMATION GATHERING AUDIT CONSIDERATIONS

General Information

EC activities to be covered:

- Describe the entity's electronic commerce activities.
- What goods / services are being sold / provided?
- Who is the typical customer?
- What is the typical form of payment?
- What is the Web site URL?
- Who is responsible for controlling these activities
  - What is their organisation reporting relationship to the entity's management?
- How long has the entity been selling such goods and services through this form of electronic commerce?
- If the electronic commerce activities have changed describe the nature of such changes
  - When did each change occur?

- Information Systems Used to Support the Electronic Commerce Activities (if not covered through the IT information gathering as highlighted in 3.1.1.1 above).

Control Environment

Describe the factors in the entity's organisation that contribute to a control environment that is generally conducive to reliable business practice disclosures on its Web site.

Describe the effective controls over electronic commerce transaction integrity and the protection of related private customer information. Such factors might include, but not be limited to:

- Management's strategy for EC;
- Hiring, development, and retention of competent personnel;
- Emphasising the importance and responsibilities for sound business practices and effective control;
- Supervising business activities and control procedures;
- Employing a suitable internal auditing function that periodically audits matters related to the entity's electronic commerce activities;
- Other factors.

Business Practice Disclosures

Describe the entity's business practices related to EC payments. How are such practices disclosed to customers? Consider the following:

- The terms and conditions by which electronic commerce transactions are conducted;
- Payment terms, including customer options, if any;
- Electronic settlement practices and related charges to customers;
- How the customer may cancel recurring charges, if any;
- Other relevant terms and conditions, if any.
- Who is responsible for controlling these activities?
- Has the entity changed its business practices or the related disclosures since the last review? If so, describe the nature of such changes and when each change occurred.

- Describe the entity's process for monitoring customer claims and complaints and for identifying patterns of claims and complaints that are not being satisfactorily addressed. A review of customer complaints may indicate weaknesses in the system.
- Describe the processes management uses to monitor the continuing effectiveness of its disclosure of business practices.

Transaction Integrity Controls

Describe the controls maintained by the entity to ensure the integrity of electronic commerce transactions. The IS auditor should describe the following.
How the entity provides reasonable assurance that:

- Each order is checked for accuracy and completeness;
- Positive acknowledgment is received from the customer before the order is processed.
- Services and information are provided to the customer as agreed to on the order;
- Back order and other exceptions are promptly communicated to the customer.
- Sales prices and all other costs are displayed for the customer before requesting acknowledgment of the order;
- Orders are billed and electronically settled as agreed;
- Billing or settlement errors are promptly corrected.
- The entity maintains controls that allow for subsequent follow-up of orders.
- Responsible has been assigned for controlling these activities.
- If the entity changed its controls over transaction integrity since the last review and if controls over transaction integrity have changed, the nature of such changes and when each change occurred are detailed.
- The processes management uses to monitor the continuing effectiveness of its controls over transaction integrity are adequate.

Information Protection Controls

Private customer information includes personal identification information for the customer or his or her family (name, address, telephone number, social security or other government identification numbers, employer, credit card numbers, etc.), personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records or

similar information. The following should be considered by the IS auditor during the information gathering phase:

- Describe the steps taken to ensure the protection of private customer information.
- Describe the controls maintained by the entity to protect transmissions of private customer information over the Internet from unintended recipients.

- Describe the controls maintained by the entity to protect from outsiders private customer information obtained as a result of electronic commerce and retained in its system.

    - How systems that retain private customer information, obtained as a result of electronic commerce, are protected from outside access.
    - How the entity ensures that customers entering through the Web page can only perform inquiries, execute authorised transactions, and obtain information about their own transactions.
    - How private customer information obtained as a result of electronic commerce is protected from intentional disclosure to parties not related to the entity's business unless:
        - customers are clearly notified prior to their providing such information, or
        - customer permission is obtained after they have provided such information.
    - How the entity ensures that private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business.

- Describe the controls maintained by the entity to protect against its unauthorised access to customer's computers and its unauthorised modification of customer's computer files:

    - How the entity ensures that customer permission is obtained before storing, altering or copying information in the customer's computer (including the use of "cookies" stored on the customer's computer system), or that the customer is notified with an option to prevent such activities;
    - How the entity ensures that transmission of computer viruses to customers is prevented;

- Who is responsible for controlling these activities?

Has the entity changed its controls over information protection since the last review? If so, describe the nature of such changes and when each change occurred.
Describe the processes management uses to monitor the continuing effectiveness of its controls over information protection.

Describe any other matters that would be relevant in evaluating EC payment security. Examples include:

- Significant changes in the entity's business or its organisational structure;
- Significant processing or controls problems with the entity's electronic commerce systems or supporting infrastructure;
- Instances of fraud and breaches of transaction integrity, security and information protection controls involving:
  - employees with electronic commerce responsibilities;
  - contractors and others who provide services to the entity related to its electronic commerce activities;
  - unauthorised third parties, or
  - systems and supporting infrastructure used for executing electronic commerce transactions.
- Significant changes in management and other key personnel with electronic commerce responsibilities.
- Other relevant information.

3 EC DETAILED AUDIT PROCEDURES AND CONTROL CONSIDERATIONS

3.1 SECURITY POLICY, CORPORATE INFORMATION SECURITY (CIS) AND SECURITY ADMINISTRATION

3.1.1 Security Policy

A security policy, Corporate Information Security Office (CISO), or security administration review would normally be performed as a separate audit. The IS auditor should ensure that aspects related to EC have been included in such previous audits. The IS auditor should therefore ensure that aspects mentioned in

this section have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

A security policy needs to lay out, in writing, the security steps followed by an organisation and should outline the issues of who, what, when, how, and why of ongoing actions and procedures. It should be a detailed document that identifies risks, defines steps taken to reduce them to acceptable levels, and outlines the tasks and job-descriptions of those directly involved in the enforcement of security in an organisation.
The auditor needs to determine whether formal security policies and security standards documents are tailored specifically for each networking environment. The auditor must also determine whether periodic assessment of systems, policies, and procedures is performed, (thereby providing an effective augmentation of existing security programs), and the implementation of new security measures and countermeasures.

Audit Procedures
Review documentation, and/or interview appropriate personnel to determine whether the CISO has performed an assessment of the risk and determined the security requirements and operational procedures to be included in the applicable Security Policy, Certificate Policy and/or Certificate Practice Statement (CPS – as used by a Certification Authority (CA)).

Ensure review document includes descriptions of the following controls:

- Primary controls including:
  - Security Policy and Security Organisation
  - Asset Classification and Control
  - Personnel Security
  - Physical and Environmental Security
  - Computer and Network Management
  - System Access Control
  - Systems Development and Maintenance
  - Business Continuity Planning
  - Legal Compliance

- Event Journal

- Key management life cycle controls including:
  - Key Generation, Storage, Backup and Recovery
  - Key Distribution, Escrow, Usage, Destruction, and Archival

- Certificate life cycle controls including:
  - Initial Certificate Registration
  - Subsequent Certificate Renewal and Rekey
  - Certificate Issuance, Distribution, Revocation, and Suspension
  - Certificate Revocation List (CRL) Processing

- Device life cycle controls including:
  - Device Shipment, Receipt, Pre-Use, Storage, Installation, Usage, De-installation, Service and Repair, and Device Retirement

Review documentation, and/or interview appropriate personnel to determine whether documented policies and procedures exist and are followed for making available the CA's Certification Practice Statement (CPS), and applicable public CA Certificate Policies to all End Entities and Relying Parties.

Interview the organization's information security manager, if someone has been appointed to that position, or other employees who have been given information security management responsibilities to determine whether their understanding of their assigned tasks is consistent with the organisation's security policy statement.

3.1.2 Security Organisation

Audit Procedures

The IS auditor should consider performing the following procedures to determine whether the requirements of the information security infrastructure, as stated in the applicable security-related documentation, are being achieved:

- Obtain documentation of the security organisation;
- Obtain and review documentation of the security related roles and responsibilities;

- Match the defined security roles and responsibilities with the names of the personnel performing the specific functions and determine whether the segregation of duties is adequate;
- Review the authorisation process for the IT facilities;
- Interview relevant personnel including the security officer;
- Obtain a copy of any reviews of the security organisation whether Internal audit, External audit, or other third party organisations, and evaluate for discrepancies found.

The IS auditor should consider performing the following procedures to determine whether the requirements for third party access, as stated in the applicable security-related documentation. are being achieved:

- Review documentation and interview appropriate personnel to determine the business need for providing third party access, if such access is allowed.
- Review documentation and interview appropriate personnel to determine the extent of third-party access allowed.
- Obtain documentation of the procedures for granting, controlling and monitoring third-party access.
- Obtain a copy of relevant Service Level agreements and review the security section to identify security considerations in the contract and ensure it has been adequately defined.
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for security reviews of IT systems, as stated in the applicable security-related documentation, are being achieved:

- Obtain reports of internal or external reviews of the IT systems against the company security policy and identify any weaknesses related to the EC payment security audit.
- Obtain reports of internal or external reviews of the IT facilities against the security implementation standards and identify any weaknesses related to the EC payment security audit.
- Evaluate the protection of system audit tools
- Interview appropriate auditors.

3.1.3 System Administration and Access Control

Audit Procedures

The auditor should consider performing the following procedures to determine whether the user access management requirements, as stated in the applicable security-related documentation, are being achieved:

- Review the user access management policy and procedure documentation;
- Interview appropriate personnel;
- Review user registration and de-registration procedures;
- Select a sample of employees who have changed jobs or left the organisation and assess the timeliness of the required changes to their access rights.
- Review privileged use log reports: determine whether the logs are reviewed and follow up actions defined and taken, where required;
- Review password management policies and procedures and determine whether they adhere to generally accepted standards;
- Review documentation to determine whether the assigned permissions and separation of duties for the Root CA systems are appropriate;
- Review documentation of the CA functions, the performance of which requires the concurrent participation of two or more individuals, and the related access lists;
- Select a sample of user accounts and test whether their access privileges are correct;
- Review policies and procedures and interview appropriate personnel to determine whether users' access rights and privileges are periodically reviewed.

The auditor should consider performing the following procedures to determine whether the requirements for user responsibilities, as stated in the applicable security-related documentation, are being achieved:

- Review password management policies and procedures;
- Interview appropriate personnel to determine whether password change requirements are in operation;

- Test the corporate and CA's documented password strength controls through review of operating system security policy criteria for passwords (e.g., format, length, history, etc.);
- Review policies and procedures related to unattended user equipment;
- Observe whether automatic log-off for unattended equipment is in operation;
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the network access control requirements, as stated in the applicable security-related documentation, are being achieved:

- Obtain a network map to understand the network components and environment;
- Review network access control policies and procedures documentation and ensure it includes descriptions of the following:
  - Limited services
  - Enforced path
  - User authentication
  - Node authentication
  - Remote diagnostic port protection
  - Segregation in networks
  - Network connection control
  - Network routing control
  - Security of network services

- Interview appropriate personnel.
- Perform automated scans of selected servers to ascertain whether known vulnerabilities are present. Review active services on the critical networks and compare it to the requirements specified in the security policy. Obtain justification for active services and evaluate for appropriateness.

The auditor should consider performing the following procedures to determine whether the computer access control requirements, as stated in the applicable security-related documentation, are being achieved:

- Review computer access control policy documentation and ensure it includes descriptions of the following computer access control requirements:

- Automatic terminal identification
- Terminal log-on procedures
- User identifiers
- Password management system
- Duress alarm to safeguard users
- Terminal time-out
- Limitation of connection time.

- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the application access control requirements related to EC payment applications, as stated in the applicable security-related documentation, are being achieved:

- Review the application access control policy and procedures documentation and ensure it includes descriptions of the following application access control requirements:

  - Information access restriction.
  - Use of system utilities.
  - Access control to program source library.
  - Sensitive system isolation.

- Interview appropriate personnel;
- Observe whether sensitive systems are physically and logically isolated;
- Observe whether the equipment in the Root CA or any encryption key generation ceremony room is not connected to any network outside of the room, is password protected and is physically secured inside the locked room.

The auditor should consider performing the following procedures to determine whether the requirements for monitoring system access and use, as stated in the applicable security-related documentation, are being achieved:

- Review the policies and procedures documentation for monitoring system access and use;

- Review configurations of logging hosts and logged clients and determine whether logging information is being produced and archived for review by management;
- Review a sample of system availability reports and determine whether they are produced on a regular basis;
- Interview management to gain an understanding of review and follow-up procedures;
- Review management reports to determine whether appropriate network monitoring information is summarised and reported to management.

Monitoring activities related to intrusion detection is covered under Section 2.11.

3.2 PHYSICAL AND ENVIRONMENTAL SECURITY

A really solid network defense is not complete if someone can physically gain access to equipment or private networks. A physical and environmental security review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that needs to be taken into account and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified during a physical or environmental security audit, the IS auditor should assess whether such weaknesses impact upon the EC payment security audit and assess management actions taken since the last audit/ review.

Audit Procedures

The auditor should perform the following procedures that relate specifically to the physical security of the EC payments security environment:

- Ensure equipment has several layers of physical security. Some examples to be considered:
  - Controlled access to the building;
  - A secure network room;
  - Locked cabinets for the equipment;
  - A screen to prevent wireless communications from leaving the room.

- Ensure E-commerce servers are located in a secured building and were included as part of the previous audit procedures for physical and environmental security. Physical security aspects should be specified in the policies and procedures documentation.

The following apply to secure areas related to CA activities.

- Ensure data centres and computer rooms supporting critical business activities have strong physical security, which includes the following:

    - Root CA operations are conducted in a physically secure environment requiring dual control;
    - Subordinate CA operations are conducted in a secure environment comparable to a data centre requiring dual control;
    - RA operations are conducted in a controlled environment, i.e., restricted or private area.

3.2.1 Asset Classification and Control

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for asset classification and control, as stated in the applicable security-related documentation, are being achieved:

- Review asset accountabilities to determine whether owners have been assigned for all major assets;
- Review the inventory of assets and verify the procedures to ensure completeness and accuracy of these lists:

    - Information assets (e.g., databases, data files, system documentation, business continuity plans, user manuals, training materials, etc.);
    - Software assets (e.g., application software, system software, utilities, etc.);
    - Physical assets (e.g., computer and communications equipment, power supplies, air conditioning units, etc.);
    - Services (e.g., computing and telecommunications services).

- Review asset classifications for reasonableness.

3.3 OPERATING SYSTEM AND WEB SERVER CONSIDERATIONS

An operating system or web server review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account, and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review. The IS auditor should review procedures to ensure the following considerations (that should be performed by the appropriate auditee personnel), have been included in an operating system review.

- Removing default CGI scripts that are not needed - these are typically not meant for commercial use.
- The web server should utilise the minimum privileges to execute CGI scripts (for example, on a UNIX system, a web server should not execute as 'root').
- Automatic directory listing should be turned off. If this is available, the program sources could be downloaded for examination for potential vulnerabilities.
- Disabled acceptance of SSIs (Server-Side Includes). SSIs are codes embedded within HTML documents. If these are uploaded to the web server they will execute under the web server privilege.
- Restrict the directories from where CGI scripts can be executed from the web server. This is because if CGI scripts are placed in user directories, there could be security threats.
- Ensure command processors or interpreters such as Perl or command.com have not been included in CGI directories.
- Allocate sufficient memory for CGI scripts to minimise the likelihood of buffer overflows.
- Ensure CGI scripts activities are recorded in a log.
- Check for proper configuration of cookie distribution. Cookies are sent between a web server and client. This could include authentication information. If the cookies are misconfigured, an unauthorized server might be able to retrieve that

cookie, and in theory, could then try to gain unauthorized access to the original web server. In other words, check whether the "secure" value of the cookie has been set to require the browser to send the cookie only over an encrypted session.

- Check to ensure all deadly defaults for the specific application and supporting operating systems are addressed. In order to find out information on the deadly defaults, one can visit the CERT sites (http://www.cert.org), vendor sites, and other security related sites such as http://www.ntsecurity.net for Windows NT.
- Turn off network services that are not needed. If the server is a mail server, http and ftp may not be needed. Opportunities for attacks increase with the number of enabled network services.
- Keep up with the latest operating system (OS) patches. These typically address potential security related OS bugs and holes that have been discovered.
- Use of strong passwords. Standard controls should apply, such as regular reviews of policies, password length and format, frequent forced change of password (e.g., every 30 days), access rights linked to staff movement, unique identifier, regular audit of the effectiveness of the procedures and applications by staff. This is also discussed in the access control Section 3.3.1.1.3.
- Document what is installed and monitor for any changes.
- Run logging and monitor log files. Actions of users should be logged and reviewed.
- Block the ability to know OS and web server information.
- Limit access to the system. Proper authentication techniques are vital. This can come down to having users log onto the system with their own user IDs (never directly as root or administrator) and care being taken to ensure proper authority levels are granted. Different authentication schemes can be utilised such as Kerberos, Radius or LDAP but it comes down to enforcing logins with proper privileges and enforcing strong password usage. Care should also be taken in how a login is achieved. Remote connections should always be avoided across the Internet through the use of a non-secure medium that could easily be captured and read (such as telnet).
- Keep the system up to date with latest fixes and patches. Keep up to date on Bugtraq or CERT advisories, and apply the necessary patches to ensure there is no exposure to any newly discovered vulnerabilities.
- Image, or back up the system at appropriate stages. Backup is mandatory as more reliance is placed on the electronic audit trail. Organisational requirements

should dictate the backup policy and this should be coordinated closely with a disaster recovery plan.

- Stage and test applications and systems on a staging server prior to implementation of systems, applications or changes in a production environment.
- Change default configurations that can endanger security i.e. customise the operating system to the environment where it is implemented.
- Determine whether the web server has been placed on a network that does not carry confidential traffic. This isolates the less secure systems from the secure. Making it difficult for an attacker to pick up or sniff internal traffic for valuable information. Using a firewall as previously mentioned can do this. Another option is to put all database and file servers providing web support service on a protected subnet. It is also important to disable any source routing that would allow the originator to influence routing decisions.

One component often overlooked in the various security models, methods, and protocols, is the end user's computer. No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end user's computer. That computer has stored all the digital certificates, most of the consumer's personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers, which store information in some very basic forms, even plain text. This use means the consumer's financial and banking data is only as secure as that computer. To further complicate matters, there are many laptop computers used at home and in business. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data. Controls that can minimise this risk are physical security, access controls and policies as described in the sections above.

3.4 CHANGE MANAGEMENT

A change management review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that need to be taken into account and audit procedures that need to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in previous audit procedures. Where weaknesses were identified, the

IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

The auditor should consider performing the following procedures. [Pieter, format appears awkward / inappropriate - needs to be inset or bulleted and the current bullets set in further.]

- Evaluate procedures that ensure that there are approval processes for upgrades and for the implementation of new systems;
- Evaluate control over the segregation of duties between the development staff and operational staff;
- Ensure separate logical development and production environments.

- Describe the entity's controls over changes to its electronic commerce business practices, its transaction integrity controls, its information protection controls, and its electronic commerce systems and supporting technology, which are designed to provide reasonable assurance that:

    - All such changes are approved by management;
    - Changes in business practices are reflected in modified disclosures of such practices;
    - Changes in the manner in which electronic commerce transactions are executed are reflected in modified business practice disclosures;
    - Controls over transaction integrity and information protection continue to function effectively;
    - The corporate security function is aware of all major changes and specify their requirements for all changes that may affect the security environment.

3.5 BUSINESS CONTINUITY PLANNING (BCP)

Audit Procedures

A BCP review would normally be performed as a separate audit. The purpose of this section is not to provide a complete audit program to cover all the aspects used for control purposes, but rather to provide considerations that needs to be taken into account and audit procedures that needs to be performed by the IS auditor. The IS auditor should ensure that aspects mentioned in this section have been included in

previous audit procedures. Where weaknesses were identified, the IS auditor should assess whether such weaknesses impact the EC payment security audit and assess management actions taken since the last audit/ review.

The auditor should consider performing the following procedures to determine whether the requirements for business continuity planning, as stated in the applicable security-related documentation, are being achieved:

- Any current BCP should address specific e-commerce needs. Determine whether plans are benchmarked with plans of similar organisations or environments. If information about similar organisations is available compare the BCP with those plans. Identify discrepancies;
- Determine whether backups recovery procedures are tested regularly and stored off-site;
- Review the emergency procedures included in the Information Systems Department's disaster recovery plan for completeness of coverage of all of the emergencies that may occur at a data processing site;
- Review the Information Systems Department's list of critical computer resources and determine if it includes e-commerce resources;
- Review documentation to determine whether business continuity planning includes disaster recovery processes for all critical components of a CA system, including the hardware, software and keys;
- Observe whether cryptographic hardware and other keying material is stored securely in vaults requiring dual access;
- Observe whether a locking cage has been employed around dedicated equipment at the hotsite data centre facility.

The auditor should consider performing the following procedures to determine whether the requirements for key compromise, as stated in the applicable security-related documentation, are being achieved:

- Review the procedures to respond to all known or suspected key or critical security component compromises;
- Ensure that disaster recovery procedures include the revocation and re-issuance of all certificates that were signed with the CA's private key in the event of the compromise or suspected compromise of a CA's private key;

- Ensure that procedures are in place for the secure and authenticated revocation of all certificates issued by the CA in the event that a CA has to replace its private key;
- Review the contingency plan for key compromise and determine whether it includes who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, encrypted data, etc;
- Interview appropriate personnel.

Note: Key compromise is considered one type of "disaster." CA termination is included under business continuity planning, because in the event the CA terminates, policies and procedures should be in place to ensure the continuity of service to customers.

The auditor should consider performing the following procedures to determine whether the requirements for CA termination, as stated in the applicable security-related documentation, are being achieved:

- Review CA termination policies and procedures to minimise potential disruptions as a result of the cessation of their services.
- Interview appropriate personnel.

3.6 ORGANISATIONAL STRUCTURE

Audit Procedures

The auditor should consider performing the following procedures to determine whether the personnel security requirements for job definition, hiring, and training, as stated in the applicable security-related documentation, are being achieved:

- Conduct interviews with human resources management to gain an understanding of the policies and procedures regarding hiring, termination, and related HR processes;
- Examine job descriptions of staff involved in EC payment security activities and assess segregation of duties;

- Review screening reports for staff involved in EC payment security activities and assess adequacy;
- Review confidentiality agreements and ensure they are signed by all staff;
- Review a sample of new hires and the background check log to determine whether background checks have been completed;
- Review a sample of "trusted employees" and confirm whether background checks have been performed;
- Review a sample of recent terminations against the badge access listing and/or network access listing to determine whether access has been cancelled and appropriate exit procedures performed;
- Review training program materials to determine whether key staff receive training related to their functions and cross training is encouraged.

The auditor should consider performing the following procedures to determine whether the security requirements for incident response, as stated in the applicable security-related documentation, are being achieved:

- Review incident reporting and response policies and procedures;
- Review the incident categorisation/classification scheme;
- Review a sample of reported incidents and determine whether incident response policies and procedures were followed;
- Interview personnel responsible for incident reporting and incident response;
- Review logs and reports of disciplinary measures taken;
- Interview personnel responsible for the disciplinary process.

The audit procedures related to intrusion detection are covered in more detail in Section 2.10 below.

3.7 COMPUTER OPERATIONS AND BACKUP

The auditor should consider performing the following procedures to determine whether the requirements for computer operations, as stated in the applicable security-related documentation, are being achieved:

- Review the documented procedures for computer operations to ensure it includes operating procedures and incident management procedures;

- Interview appropriate personnel to determine segregation of duties and separation of development and operational facilities;
- Determine whether any external facilities are used. Evaluate procedures related to this service.

The auditor should consider performing the following procedures to determine whether the requirements for system planning and acceptance, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the system planning and acceptance process and ensure the following activities are included:
- Capacity planning
- System acceptance
- Fallback planning
- Operational change control (also covered in change control above)
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for virus control, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of virus control policies and procedures and ensure it also includes user awareness procedures, regular virus software update and scanning procedures, and virus detection emergency procedures;
- Interview appropriate personnel.

The auditor should consider performing the following procedures to determine whether the requirements for data backup, operator logs and monitoring, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the processes for data backup, operator logging and monitoring;
- Interview personnel responsible for data backup to gain an understanding of the adequacy of the procedures used to back up the computer system and to maintain and store computer magnetic tapes. Ensure that it includes EC systems;

- Review selected sections of the backup procedures manual and determine whether the procedures are properly documented;
- Select a sample of tape volume serial numbers for EC related backups from the backup tape listing and compare tape serial numbers to the physical tape residing in the tape library to determine whether the tapes are properly accounted for and recorded;
- Obtain and read the contract with the off-site storage vendor, if applicable, to determine whether responsibilities are clearly outlined, and whether a list of authorised personnel is maintained and current;
- Review the backup logs and configuration files for servers (including EC servers such as the web server) to determine whether they are backed up regularly and properly.
- Review documents to determine whether expired and/or defective tapes are destroyed in a controlled manner.

- Ascertain the requirements for network security control, as stated in the applicable security-related documentation, that should at least include descriptions of the following network security control requirements:

    - Ensure there is separation of operational responsibilities for networks from computer operations, where appropriate;
    - Evaluate responsibilities and procedures for the management of remote equipment, including equipment in user areas;
    - Assess controls to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems i.e., ensure encryption, secure protocols and digital certificates are used where applicable;
    - Assess co-ordination of computer and network management activities to optimise system performance and to ensure the consistency of security measures across the IT infrastructure.

3.8 FIREWALL AND ROUTER CONSIDERATIONS

The role of the IS auditor in this respect is to ensure that the firewall/ router review policy covers the following controls and procedures:

- Obtain network diagrams and understand the architecture of the network and the nature and location of network firewalls and routers. The auditor should consider performing the following procedures:

    - Determine the environment in which the firewalls and routers operate. Discuss with management their assessment of the relative hostility of the environment;
    - Obtain an understanding of the role that firewalls and routers play in the network (e.g., Do routers simply provide connectivity or do they also provide control?);
    - Examine the network architecture and identify where firewalls and routers play a role in authentication and authorisation;
    - Understand how changes to the network are initiated and managed and ensure that all changes are approved and monitored.

- Determine whether remote firewall and router administration is avoided, especially over the Internet. The firewall/router also needs to be securely managed to limit the possibility of someone breaking into it. As the protector of the network, the router or firewall is a target for intruders. Managing the firewall/router via the Internet interface is probably the least desirable situation, especially if the management connection is of questionable encryption strength or can be spoofed. Taking care not to allow management ports to be available to the Internet also helps prevent fingerprinting the type of firewall/router used;
- Ensure firewall/router software is upgraded on a regular basis, with patches and upgrades. For software-based firewalls, this applies to the operating system and the firewall software;
- Ensure firewalls/routers are reviewed periodically e.g., through the use of commercial products that can help make this task easier such as the Internet Security Scanner ISS - http://www.iss.net;
- The auditor should consider performing the following procedures related to auditability of routers and firewalls:

    - Through discussion and review of available documentation, determine whether the firewalls and router management and security activity records are being maintained;
    - Ensure that the records are adequate for the needs of the organization;

- Understand the monitoring and review activities performed by network management;
- Ensure that logs are properly configured, monitored, and audited. The firewall product will deny access to unauthorized connections, will show where those attempts originated and what ports they were destined to. There are many types of firewalls that can exist on the host. There are also firewalls that are used to protect networks;
- Determine if information gathered from logs is used to find patterns, misconfigured equipment and break-in attempts. This information can be used to communicate those attempts to the owners of the originating hosts.

- As with most operating systems, firewalls and routers never come out-of-the-box configured to secure any given site, and are only as good as the staff administrating them. Evaluate skills and segregation of duties for staff administering the firewalls. The auditor should consider performing the following procedures:

  - Determine how firewalls and routing tables are created and maintained;
  - Determine how changes to firewalls and routing tables are managed and controlled and whether the control of these changes is limited to a single person at a time;
  - Determine how this person is authenticated;
  - Through discussion with management, understand the types of services and network components to which access is intended to be granted;
  - Review the access tables to determine what access they are providing and the filters used. Document any services which were not intended / authorised;
  - Review the network architecture and the firewalls and routing tables of selected firewalls/routers to determine whether the concept of "least cost path routing" is applied.

- Determine whether filters are as specific as possible. Permissions for inherently dangerous traffic, such as rules that allow remote management, should always be as specific as possible. But less obvious threats are often overlooked;

- If different systems are used for web site and mail, ensure web and mail traffic are not allowed to the entire subnet. Specify mail traffic allowed to the mail server and web traffic to the web server;
- Allowing SMTP traffic to a web server may not seem to be all that large a risk, but it is an unnecessary one: i.e., evaluate whether SMTP traffic is needed;
- The auditor should consider performing the following procedures regarding changes to firewalls and routers:

    - Understand how "read" vs. "read and update" access is granted to the firewalls and router tables;
    - Understand the source of changes to the firewalls, routing, and security tables, whether from a local console only, or from the network as well;
    - If changes can be made from the network, determine how the firewall/router is protected from interference and contamination;
    - If a password is used to control update access, determine who has access to it and how it can be changed;
    - Determine if changes to firewalls and router tables are approved by management and logged;
    - Determine if accountability for changes is maintained to the level of a single individual;
    - Through discussion with management and review of available documentation, understand the population of users that should be granted access by the routers;
    - Review the access tables to determine the definition of the access paths granted and the type of access allowed. Network users should be routed to the specific devices that they are intended to have access to. Document any access which is not intended;
    - Through discussion with management and review of available documentation understand the authentication methods used;
    - Some routers have an alternate access path defined, a dial-in access port. Look at how that is controlled. In particular, if they are using the router as a firewall or some significant security device, determine if a secure id or one-time password is used to access that port, or if the connection is manually controlled.

- The auditor should consider performing the following procedures regarding recoverability of firewalls and routers:

  - Based on our understanding of the network architecture, determine the established firewalls and router redundancy, and the adequacy of the firewall/router configurations to minimize disruption in the event of a problem;
  - Through discussion with management, determine whether a plan has been established for recovery of a single router or multiple routers;
  - Review the recovery plan to ensure it is up-to-date and adequate to address the specific recovery needs of the company;
  - Ensure that the router management techniques and tools provide easy reconfiguration of firewalls and routers in the event they go down.

- The auditor should consider performing the following evaluative procedures on the techniques and tools used for management of the routers and firewalls:

  - Through discussion with management and review of available documentation, determine the techniques and tools used for management of the routers and firewalls;
  - Determine if the procedures are documented;
  - Based on the tools used, ensure that known risks and weaknesses are adequately addressed by the client;
  - Discuss with the network managers the adequacy of the tools to facilitate easy firewall and router configuration;
  - Understand the controls over the password that allows the network manager to control the firewall or router device; ensure that is not easily guessed and is frequently changed to ensure that routers cannot be turned on or off or configurations changed without management approval.

3.9 ENCRYPTION, PRIVACY, AND SECURE PROTOCOLS

One of the objectives of encryption and secure protocols is to ensure information protection, i.e., ensure that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business. Primary considerations that should be evaluated by the IS auditor include the following:

- Controls to protect private customer information obtained as a result of electronic commerce and retained in its system from outsiders. For example, customers entering through the Web page can only perform inquiries, execute transactions and obtain information about their own transactions. The auditor can ensure this is controlled by ensuring that all system access from outside the entity, other than for customary electronic commerce transactions through the Web page, (through the Internet, dial up, or other connections) is restricted by one-time passwords and smart cards. This has also been covered in the access control section above.
- Private customer information obtained as a result of electronic commerce is not intentionally disclosed to parties not related to the entity's business unless (1) customers are clearly notified prior to their providing such information or (2) customer permission is obtained after they have provided such information.
  - In some cases, customers may be asked for explicit permission to provide their private information to other parties, and customers have the option to decline. Ensure the entity has a systematic way of identifying those customers who have not granted such permission and ensuring that their private information is not provided to other parties.
  - Determine whether customers are informed when certain requested information is optional and are not required to furnish such information to complete the transaction.
  - Determine whether certain private customer information maintained is encoded to make it extremely difficult, but not impossible, for outsiders to understand it without the appropriate codes and keys.
- Private customer information obtained as a result of electronic commerce is used by employees only in ways associated with the entity's business:
  - Determine whether the entity has strict policies and monitoring procedures to ensure that only certain employees can access private customer information. These policies also set forth ways that customer information should and should not be used.
- The entity maintains controls to protect against its unauthorised access to customer's computers and its unauthorised modification of customer's computer files by ensuring that customer permission is obtained before storing, altering or copying information in the customer's computer or the customer is notified with an option to prevent such activities:

- Evaluate whether the entity requests the customer's permission before it intentionally stores, alters or copies information (such as cookies and other similar files) in the customer's computer;
- Determine whether the entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer, and evaluate controls related to this process.

The IS auditor should evaluate controls to ensure that:

- Private customer information is protected during transmission by using encryption technology (Secure Sockets Layer (SSL) technology);
- The entity has registered its Domain Name and Internet IP address to protect its Internet identity. The address is unique and no more than one company can have the same address;
- The entity's Web page has a digital certificate which can be checked using features in a standard Web browser. Certificates are covered in detail in the PKI section below;
- The entity's Webmaster updates the site and reviews and tests key Web pages at least daily to ensure that improper content or links have not been added;
- SSL has been configured with the systems software according to the vendor recommendations;
- The entity uses a standard web browser version that supports SSL encryption.

The IS auditor should attempt to obtain a connection to the entity's web site and observe whether SSL is activated when private information and payment information is collected from customers. This would also verify the certificate issuing process.

The aspects related to encryption keys and digital certificates are addressed in the PKI section below.

3.10 PKI AUDIT AND CONTROL CONSIDERATIONS

3.10.1 Key Management Life Cycle Controls

3.10.1.1 Key Generation

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key generation, as stated in the applicable security-related documentation, are being fulfilled:

- Obtain documentation of the cryptographic modules used for key generation;
- If cryptographic modules are internally developed (and internally tested) without external third-party evaluation, consider the functional correctness of the cryptographic module;
- If cryptographic modules are externally tested, obtain a copy of the evaluation report and/or verify the module's FIPS 140-1 certification at the manufacturer's URL i.e.:
  - Root CA key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 4 requirements;
  - Sub-CA and RA key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 3 requirements;
  - End Entity key generation occurs within a secure cryptographic device meeting the FIPS 140-1 Level 2 requirements;
  - Review the configuration of the cryptographic module and compare it with the configuration specifications provided by the vendor and/or test lab;
  - Observe a key generation ceremony and related event journals (audit trails) produced to ascertain whether key generation ceremony procedures are followed. This may include:
    - Key generation uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard;
    - Key generation uses a prime number generator as specified in an ANSI X9 or ISO standard;
    - Key generation uses a key generation algorithm as specified in an ANSI X9 or ISO standard;
    - Key generation results in key sizes in accordance with the CA's CPS;

- The key generation process takes place in a physically secure environment;
- Key generation takes place with dual control.
- Observe whether cryptographic hardware is tested before key generation;

- Interview appropriate personnel that perform key generation.

3.10.1.2 Key Storage, Backup and Recovery

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key storage, backup and recovery, as stated in the applicable security-related documentation, are being fulfilled:

- Review documentation of the key storage, backup and recovery processes and ensure that:
  - If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of off-lineoff-line processing or backup and recovery, then the CA private key is generated and used within the same cryptographic module and is never exported outside of the cryptographic module.
  - If the CA private key is exported from a secure cryptographic module and moved to secure storage for purposes of off-line processing or backup and recovery, then the private key is exported in a secure key management scheme including:
    - as ciphertext using dual control,
    - as encrypted key fragments using dual control and split ownership, or
    - in another secure cryptographic module such as a key transportation device using dual control.
- For storage in a cryptographic module:
  - If the Root CA private key is stored as cleartext, then the Root CA private key never appears as cleartext outside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 4 requirements;
  - If the Root CA private key is stored as ciphertext, then the Root CA private key is stored inside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 3 requirements;

- If the Subordinate CA or RA private key is stored as cleartext, then the Subordinate CA or RA private key never appears as cleartext outside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 3 requirements;
- If the Subordinate CA or RA private key is stored as ciphertext, then the Subordinate CA or RA private key is stored inside the secure confines of a cryptographic module meeting at least FIPS 140-1 Level 2 requirements.

- Recovery of the CA private key is conducted in the same secure scheme used in the backup process, using dual control;
- The integrity of the CA private key is maintained throughout its life cycle;
- Observe the key storage, backup and recovery process;
- If approved cryptographic modules are used for the storage, backup and recovery of private keys, determine whether test lab documentation is current;
- Interview appropriate personnel who perform key storage, backup and recovery operations.

The auditor should consider performing the following procedures to determine whether the management controls for key storage, backup and recovery, as stated in the applicable security-related documentation, are being adhered to:

- Review documentation of the key storage, backup and recovery process and ensure the following
  - Ensure that the private key is backed up, stored and recovered using dual control in a physically secured environment;
  - Ensure that private key storage and recovery is performed only by authorised personnel;
  - Verify that recovery is to a cryptographic module, in which:
    - The Root CA private key is accessed and imported for purposes of off-line processing or backup and recovery into a cryptographic module meeting the requirements of FIPS 140-1 Level 4 using dual control in a physically secure site;
    - The Subordinate CA private key is accessed and imported for purposes of off-line processing or backup and recovery into a cryptographic module meeting the requirements of FIPS 140-1 Level 3 using dual control in a physically secure site.

- Verify that the backup and recovery period for private and public keys is in accordance with the applicable security-related documentation;
- Verify that backup and recovery procedures are tested on a periodic basis in accordance with the applicable security-related documentation;
- Verify that key storage, backup and recovery actions are recorded in the event journal;
- Observe the key storage, backup and recovery process;
- If approved cryptographic modules are used for the storage, backup and recovery of private keys, determine whether test lab documentation is current;
- Interview appropriate personnel that perform key storage, backup and recovery operations.

3.10.1.3 Key Distribution

This section covers the distribution of the Root CA public key. The distribution of non-Root CA public keys is covered in Certificate Distribution.

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key distribution, as stated in the applicable security-related documentation, are being fulfilled:

- Review documentation of the process for the periodic rekeying of the Root CA and ensure the Root CA public key must be changed (rekeyed) periodically according to the requirements of the applicable CA Certificate Policy and/or CPS.
- Review documentation of the process for the initial distribution of the Root CA public key and ensure the integrity and authenticity of the key and associated parameters are maintained.
- Review documentation of the process for the subsequent distribution of the Root CA public key.
- Review a sample of event journals to determine whether key distribution actions are properly recorded.
- Interview appropriate personnel.

3.10.1.4 Key Escrow

Key escrow refers to the process whereby law enforcement officials can gain access to an escrowed private key.

Audit Procedures

Determine whether the requirements for key escrow, as stated in the applicable security-related documentation, are being fulfilled. The auditor should consider performing the following procedures:

- Review documentation of the storage, backup and recovery controls and procedures of the third party providing escrow services;
- Determine whether digital signature keys are ever subject to key escrow, or any other form of key recovery;
- Review documentation of the CA's key escrow process.
- Review the escrow contract between the involved parties and ensure it outlines the liabilities and remedies between the parties;
- Determine whether key escrow actions by a third party are recorded in the CA's event journal when communicated to the CA;
- Interview appropriate personnel at the CA that perform the key escrow process;
- If possible, interview appropriate personnel of the third party providing escrow services that are involved in the key escrow process.

3.10.1.5 Key Usage

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key usage, as stated in the applicable security-related documentation, are being fulfilled:

- Review key usage documentation and ensure keys are only used for their intended purpose, which is specified during key generation;
- Review policies and procedures relating to key usage and ensure certificate signing is performed by the Root CA using dual control;

- Observe the authentication requirements for the activation and de-activation of the CA private key and ensure the activation of the CA private key is performed using two factor authentication;
- Review a sample of event journals to determine whether key usage actions were properly recorded;
- Interview appropriate personnel.

3.10.1.6 Key Destruction

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key destruction, as stated in the applicable security-related documentation, are adhered to:

- Review documentation of the key destruction process and ensure all copies and fragments of the CA private key are destroyed at the end of the key pair life cycle, using dual control in a physically secure site;
- Review a sample of event journals to determine whether key destruction actions were properly recorded;
- Interview appropriate personnel that perform the destruction process.

3.10.1.7 Key Archival

Audit Procedures

The auditor should consider performing the following procedures to determine whether the requirements for key archival, as stated in the applicable security-related documentation, are being achieved:

- Review documentation of the key archiving process, and ensure archived keys are periodically verified to ensure that they are properly destroyed upon expiration;
- Observe the key archiving process and ensure:

- All archived keys are destroyed at the end of the archive period using dual control in a physically secure site, as required by the applicable security-related documentation;
- Keys held in archive meet the requirements for key storage, backup and recovery;
- Mechanisms are in place to ensure that archived keys are never put back into production;
- Mechanisms are in place to ensure that the archived keys are recovered for the shortest time period technically possible;
- Private keys are archived to permit access to data after the certificate expires.
- Interview appropriate personnel that perform key archiving operations;
- Ensure the archival process includes entries into the event journal.

3.10.2 Device Life Cycle Management

For purposes of this section, "device" refers to cryptographic hardware and other hardware used for sensitive CA operations.

Audit Procedures

3.10.2.1 Device Shipment

Determine whether the requirements for device shipment, as stated in the applicable security-related documentation, are adhered to. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device shipment;
- Observe the receipt of cryptographic hardware from the manufacturer via registered mail with tamper evident envelopes and seals intact;
- If observation is not possible in the two guidelines above, interview appropriate personnel;
- Ascertain the requirements for physical protection of cryptographic hardware as stated in the applicable security-related documentation.

3.10.2.2 Device Receipt

The auditor should consider performing the following procedures to determine whether the requirements for device receipt, as stated in the applicable security-related documentation, are adhered to:

- Review policies and procedures documentation related to device receipt;
- Observe the inspection of the tamper evident packaging upon receipt of cryptographic hardware from the manufacturer;
- Observe the process of acceptance testing and verification of firmware settings;
- Observe for integrity the process of testing devices used for private key storage and recovery and the interfaces to these devices;
- For the guidelines above, if observation is not possible, interview appropriate personnel;
- For a sample of devices that have been received recently, check the event journal for the recording of the device receipt.

3.10.2.3 Device Pre-Use Storage

Determine whether the requirements for device pre-use storage, as stated in the applicable security-related documentation, are being adhered to. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to pre-use storage, and ensure that, to prevent tampering, the device is stored in a secure site, with access limited to authorised personnel. The procedures should have the following characteristics:
  - Inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device;
  - Access control processes and procedures to limit physical access to authorised personnel only;
  - All successful or failed physical access attempts are recorded in an event journal;
  - Incident processes and procedures to handle abnormal events, security breaches, and investigation and reports;
  - Audit processes and procedures to verify the effectiveness of the controls.

- Observe whether cryptographic hardware is stored in tamper resistant envelopes;
- Select a sample of cryptographic hardware tokens from the inventory listing and verify their status and location;
- Interview appropriate personnel;
- For devices entered or removed, determine whether these actions were properly recorded in an event journal;
- Ensure the handling of cryptographic hardware is performed in the presence of no less than two trusted employees.

3.10.2.4 Device Installation and de-installation

Determine whether the requirements for device installation, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device installation and de-installation;
- Observe the process of device installation and ensure the installation of cryptographic hardware is performed in the presence of no less than two trusted employees;
- For the guideline above, if observation is not possible, interview appropriate personnel;
- For a device that has been installed or de-installed, determine whether the device installation / de-installation was properly recorded in an event journal.

3.10.2.5 Device Usage

Determine whether the requirements for device usage, as stated in the applicable security-related documentation, are being achieved. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device usage and ensure they are followed:
  - to verify correct processing on a periodic basis;
  - to provide diagnostic support during trouble shooting.
- Interview appropriate personnel;

- Select a sample of device usage events and determine whether they were properly recorded in an event journal.

3.10.2.6 Device Service and Repair

Determine whether the requirements for device service and repair, as stated in the applicable security-related documentation, are fulfilled. The auditor should consider performing the following procedures:

- Review policies and procedures documentation related to device service and repair and ensure:
- The service or repair site is a secure site with inventory control and access limited to authorised personnel;
- The handling of cryptographic hardware is performed in the presence of no less than two trusted employees;
- The designation of a device for service and repair is recorded in an event journal;
- Upon the receipt of cryptographic hardware that has been serviced or repaired, policies and procedures require acceptance testing and verification of firmware settings.
- Interview appropriate personnel;
- Select a device servicing or repair event and determine whether it was properly recorded in an event journal.
-

3.10.3 Certificate Life Cycle Controls

3.10.3.1 Initial Certificate Registration

Audit Procedures

Determine whether the requirements for the certificate request, as stated in the applicable security-related documentation, are complied with:

- For the Subordinate CA initial certificate registration, the auditor should consider performing the following procedures:

- Review documentation to ascertain that the Root CA (or Superior CA) documents its requirements for the CA certificate request and makes them available to the Sub-CA;
- Interview appropriate personnel.

- For the End Entity initial certificate registration, the auditor should consider performing the following procedures:
  - Review documentation to ascertain whether the End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration information to the RA;
  - Interview appropriate personnel.

- For the initial certificate registration in general, the auditor should consider performing the following procedures:

  - If an on-line application is utilised to collect application information, obtain documentation of the on-line application processing to ascertain that:
    - The online form is adequately protected from unauthorised modification;
    - The on-line form requires completeness of information prior to submission to the registration authority (RA);
    - The submission of the application data is logically secured while in transmission.
  - If an off-line or manual application form is utilised, obtain documentation of application processing to ascertain whether the off-line form collects all relevant information, as required in the Certificate Policy, to perform the validation step;
  - Review documentation of the acceptance process and interview appropriate personnel to determine whether subscribers are required to review and accept the terms and conditions of the Certification Practice Statement and subscriber agreements prior to the submission of a certificate application;
  - If a web-wrap agreement is utilised, ascertain the method utilised to manage the changes of the related on-line subscriber agreement, reviewed and approved by the applicant as follows:
    - Review configuration management controls over online version of agreements;
    - Review event journals (audit trails) of changes to the agreements;
    - Review notifications to existing subscribers.

Determine whether the requirements for the registration (application) process, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- For the Subordinate CA registration (application) process, the auditor should consider performing the following procedures:
  - Review documentation to ascertain whether the Sub-CA submits the required certificate request information to the Root CA (or Superior CA);
  - Review documentation to ascertain whether the Sub-CA submits evidence to the Root CA (or Superior CA) that it possesses the private key corresponding to the public key;
  - Interview appropriate personnel.

- For the End Entity registration (application) process, the auditor should consider reviewing documentation to ascertain that:
  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required credentials to the RA, as well as evidence to the RA that it possesses the private key corresponding to the public key;
  - Interview appropriate personnel.

- For the registration (application) process in general, the auditor should consider performing the following procedures:

  - Interview appropriate personnel to gain an understanding of certificate request processing;
  - Review procedures manuals;
  - Observe whether online certificate enrolment requests are encrypted during transmission (e.g., using an SSL session);
  - Observe whether online certificate applications require completion of all required fields in order to be processed;
  - Select a sample of issued certificates and review the CA's issuance checklists or procedures to assess the completeness of the subscriber-provided information;
  - Re-perform the authentication process for a sample of issued certificates;

- Observe and determine whether the CA system prevents a certificate from being issued if any of the required fields is incomplete;
- Select a sample of selected certificate files and determine whether they contain appropriate retained documentation with respect to the authentication process;
- Observe and determine whether only authorised individuals are permitted access to CA systems for processing and issuance of certificate enrolment/revocation requests.
- Review a sample of the CA system logs of authentication steps by user ID, date, and time to determine whether these are complete;
- Interview CA system validation personnel and review quality control evaluations to gain an understanding of the quality control reviews of staff related to certificate issuance.

Determine whether the requirements for the registration (application) validation process, as stated in the applicable security-related documentation, are being complied with. The auditor should consider performing the following procedures:

- For the Subordinate CA registration (application) validation process, the auditor should consider reviewing documentation to ascertain that:
  - The Root CA (or Superior CA):
    - authenticates the Sub-CA;
    - authorises the Sub-CA's CA certificate request;
    - verifies the public and private key of the Sub-CA;
    - checks the data accuracy of the Sub-CA's CA certificate request.
    - when the Root CA (or Superior CA) detects duplicate public keys, the certificate request is rejected and the original certificate is revoked;
  - Interview appropriate personnel.

- For the End Entity registration (application) validation process, the auditor should consider reviewing documentation to ascertain that:

  - The RA:
    - authenticates the End Entity;
    - authorises the End Entity's registration request;
    - verifies the public and private key of the End Entity;
    - submits the required certificate request information to the CA;

- submits the required authentication data to the CA.

- The CA authenticates the RA for the registration request;
- The CA checks the data accuracy of the RA's certificate request;
- When the CA detects duplicate public keys, the certificate request is rejected and the original certificate is revoked;
- Interview appropriate personnel.

- For the registration (application) validation process in general, the auditor should consider performing the following procedures:

  - Review documentation of the certificate application validation process.
  - Ascertain whether personnel performing the certificate application validation process are adequately trained, understand their roles and responsibilities and possess the requisite skills, education and trustworthiness in accordance with the CPS as follows:
    - Review the requirements of the CP/CPS;
    - Observe personnel performing certificate application validation processing;
    - Interview appropriate personnel.

  - Ascertain whether procedures controlling the authentication of validation personnel against the certificate management system exist and are followed;
  - Review documentation of the authentication and identification procedure:
    - Interview appropriate personnel;
    - Determine the means of authentication, including digital certificates, passwords, tokens or biometrics;
    - Determine the management process for approving and updating user access lists;
    - Observe the authentication and validation procedure performed by certificate application validation personnel.

  - Review documentation and interview appropriate personnel to ascertain whether quality control procedures over the certificate registration (application) validation process exist and are followed. Specifically ascertain whether:

- An individual independent of the validation process performs periodic review of validation procedures;
- The results of such periodic reviews are summarised and presented to management in a timely manner;
- Quality control trend information is maintained and periodically reviewed to identify negative trends that require management attention or procedural changes;
- Identified errors are corrected in a timely manner;
- The results of each quality assurance review provide input into a continuous improvement process.

- Select a sample of quality control reviews performed by the CA to ascertain whether:
  - The individual performing the quality control review is independent of the validation process;
  - The results were properly summarised and reported to management;
  - Corrective action has been taken on deficiencies noted in quality control reviews.
- If a manual form is used to submit certificate application data, review controls over the integrity of data input into the certificate management system:
  - The auditor should ascertain whether the following procedures are performed:
    - manual review by the subscriber of information entered into the system;
    - secondary review by CA personnel; and/or online edit checks in co-ordination with the validation procedures.
  - The auditor should consider selecting a sample of manual forms submitted by the subscriber and compare the actual information to that entered in the system;
  - Select a sample of certificates issued by the CA and re-perform the validation steps. In doing so, consider the following:
    - validation steps documented in the CPS;
    - related system based controls to validate application data;
    - appropriateness of the source of automated validation data.
- Review documentation of the process for processing incomplete or unvalidated certificate applications;

- Observe personnel processing incomplete or unvalidated certificate applications;
- Interview appropriate personnel;
- Review documentation and interview appropriate personnel to ascertain the controls in place under which the RA validates that the subject of the certificate application has control over the private key corresponding to the public key submitted with the application;
- Review documentation of the event journal (audit trail) updating process for critical validation processing;
- Review documentation to ascertain whether the audit trail contains sufficient information to identify the individual or system responsible for performing the validation steps and approving the issuance of a digital certificate.

3.10.3.2 Subsequent Certificate Renewal

The difference between certificate renewal and the initial certificate application is that the renewed certificate contains essentially the same information and the same public key, with some minor changes (e.g., the issuance date or expiration date will change). Therefore, less information may be required to be submitted by the End Entity or the Subordinate CA.

Audit Procedures

Determine whether the requirements for certificate renewal, as stated in the applicable security-related documentation, are being fulfilled.

- For certificate renewal in general, the auditor should consider performing the following procedures:

  - Obtain documentation of the certificate renewal process and ensure it specifies the following:
    - CA only renews certificates that it previously issued;
    - The CA renews a certificate only after validating the certificate renewal request;
    - The CA or RA, if used, has a procedure for notifying subscribers prior to the expiration of their certificate of the need for renewal.
  - Select a sample of certificate renewal requests and ascertain that

- the CA validated the signature on each Certificate Renewal Data submission,
- verified the existence and validity of the certificate to be renewed; and
- verified that the request meets the specific requirements of the CPS;

- Select a sample of renewal requests and renewed certificates to ascertain that the CA has not renewed an expired certificate;
- Ascertain whether only trusted personnel are allowed to perform certificate renewal functions;
- Ascertain that the Certificate Renewal Data contains:
  - The Distinguished Name of the End Entity;
  - The Serial Number of the certificate; and
  - The requested Validity Period.

Determine whether the requirements for subsequent certificate rekey, as stated in the applicable security-related documentation, are being fulfilled:

- For Subordinate CA certificate renewal, the auditor should consider reviewing documentation to ascertain that:
  - The Root CA (or Superior CA) documents its requirements for the CA certificate renewal request and makes them available to the Sub-CA;
  - The Sub-CA submits the required certificate renewal request information, including the unexpired Sub-CA certificate, to the Root CA (or Superior CA);
  - The Sub-CA signs the CA certificate renewal request using the unexpired Sub-CA private key corresponding to the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) authenticates the Sub-CA by verifying the signed CA renewal request using the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) verifies the unexpired Sub-CA certificate;
  - The Root CA (or Superior CA) checks the data accuracy of the Sub-CA's CA certificate renewal request;
  - Interview appropriate personnel.

- For End Entity certificate renewal, the auditor should consider reviewing documentation to ascertain that:

  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration renewal information, including the unexpired End Entity certificate, to the RA

and the End Entity signs the registration renewal request using the unexpired End Entity private key corresponding to the unexpired End Entity certificate;

- The RA authenticates the End Entity by verifying the signed registration renewal request using the unexpired End Entity certificate;
- The RA authorises the End Entity's registration renewal request;
- The RA verifies the unexpired End Entity certificate;
- The RA submits the required certificate renewal request information, including the unexpired End Entity certificate, to the RA;
- The RA submits the required authentication data to the CA;
- The CA checks the data accuracy of the RA's certificate renewal request;
- Interview appropriate personnel.

3.10.3.3 Subsequent Certificate Rekey

The difference between certificate rekey and the initial certificate application is that the certificate contains the same information, with some minor changes (e.g., the issuance date or expiration date will change); however the public key is different. Therefore, less information may be required to be submitted by the End Entity or the Subordinate CA.

Audit Procedures

Determine whether the requirements for subsequent certificate rekey, as stated in the applicable security-related documentation, are achieved:

- For the Subordinate CA, the auditor should consider reviewing documentation to ascertain that:

  - The Root CA (or Superior CA) documents its requirements for the CA certificate rekey request and makes them available to the Sub-CA;
  - The Sub-CA submits the required certificate rekey request information, including the unexpired Sub-CA certificate, to the Root CA (or Superior CA);
  - The Sub-CA submits evidence to the Root CA (or Superior CA) that it possesses the new private key corresponding to the new public key;
  - The Root CA (or Superior CA):
    - Authenticates the Sub-CA by verifying the signed CA rekey request using the unexpired Sub-CA certificate;
    - Authorises the Sub-CA's CA certificate rekey request;

- Verifies the unexpired Sub-CA certificate;
- Verifies the new public and private key of the Sub-CA;
- Checks the data accuracy of the Sub-CA's CA certificate rekey request;
- Detects possible duplicate public keys, and if found rejects the certificate rekey request and revokes the original certificate.

- Interview appropriate personnel.

- For the End Entity, the auditor should consider reviewing documentation to ascertain that:

  - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity submits the required registration rekey information, including the unexpired End Entity certificate, to the RA and the End Entity signs the registration rekey request using the End Entity private key corresponding to the unexpired End Entity certificate;
  - The RA:
    - Authenticates the End Entity by verifying the signed rekey renewal request using the unexpired End Entity certificate;
    - Verifies the unexpired End Entity certificate;
    - Verifies the new public and private key of the End Entity;
    - Submits the required certificate rekey request information, including the unexpired End Entity certificate, to the CA;
    - Submits the required authentication data to the CA.
  - The CA authenticates the RA for the registration rekey request;
  - The CA checks the data accuracy of the RA's certificate rekey request;
  - When the CA detects duplicate public keys, the certificate rekey request is rejected and the original certificate is revoked;
  - Interview appropriate personnel.

- For subsequent certificate rekey in general, the auditor should consider reviewing documentation to ascertain that:

  - The CA only rekeys certificates that it previously issued;
  - The CA rekeys a certificate only after validating the certificate rekey request;
  - Certificate rekey is allowed only after performing all three of the following:
    - The CA validates the signature on the Certificate Rekey Data submission;

- The CA verifies the existence and validity of the certificate to be rekeyed;
- The CA verifies that the request, including the extension of the validity period, meets the requirements defined in the CPS.

- The CA or RA, if used, has a procedure for notifying subscribers prior to the expiration of their certificate of the need for rekey;
- Interview appropriate personnel.

3.10.3.4 Certificate Issuance

Audit Procedures

Determine whether the requirements for certificate issuance, as stated in the applicable security-related documentation, are complied with. For Subordinate CA and End Entity certificate issuance, the auditor should consider performing the following procedures:

- Review documentation of the certificate issuance process;
- Review documentation of the procedures used by the CA to ensure uniqueness of distinguished name and to determine that the public key is unique;
- Review documentation to determine whether the CA generates X.509 version 3 certificates with key usage fields, validity periods and extension fields in accordance with the proper X.509 version 3 syntax;
- Review documentation to determine whether the issuing CA verifies its own digital signature for the certificate;
- Interview appropriate personnel.

Determine whether the requirements for certificate distribution upon subscriber acceptance, as stated in the applicable security-related documentation, are complied with. For Subordinate CA and End Entity certificate issuance, the auditor should consider performing the following procedures:

- Review documentation of the certificate distribution process (e.g., process for updating the certificate repository);
- Review documentation to determine whether certificates are distributed only upon subscriber acceptance;

- Determine the means of subscriber acceptance and develop tests of controls or substantive tests as appropriate;
- Interview appropriate personnel.

Determine whether the requirements for certificate receipt and verification by the subscriber, as stated in the applicable security-related documentation, are fulfilled.

- For Subordinate CA certificate issuance, the auditor should consider reviewing documentation to determine whether:

    - The Root CA sends the required certificate response data to the Sub-CA;
    - The Sub-CA authenticates the Root CA (or Superior CA);
    - The Sub-CA checks the data accuracy of the certificate;
    - The Sub-CA verifies the certificate;
    - Interview appropriate personnel.

- For End Entity CA certificate issuance, the auditor should consider reviewing documentation to determine whether:

    - The CA sends the required certificate response data to the RA;
    - The RA authenticates the CA;
    - The RA matches the certificate response to the original registration request;
    - The RA sends the required registration response data to the End Entity;
    - The End Entity checks the data accuracy of the certificate;
    - The End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity verifies the certificate;
    - Interview appropriate personnel.

If required by the applicable CA Certificate Policy, determine whether the requirement for the CA to notify the subscriber of the issuance of a certificate in an out-of-band communication, as stated in the applicable security-related documentation, is complied with.

- For Subordinate CA certificate issuance, the auditor should consider performing the following procedures:

    - Review documentation of the out-of-band communication process;
    - Assess the strength of the out-of-band communication process;

- Select a sample of certificates issued and review the out-of-band communication for each certificate;
- Review documentation to ascertain whether the Sub-CA system (hardware, software, etc.) operates according to specifications such that the Sub-CA handles the out-of-band notification from the Root CA;
- Interview appropriate personnel.

- For End Entity certificate issuance, the auditor should consider performing the following procedures:

  - Review documentation of the out-of-band communication process;
  - Assess the strength of the out-of-band communication process;
  - Select a sample of certificates issued and review the out-of-band communication for each certificate;
  - Review documentation to ascertain whether the End Entity system (hardware, software, etc.) operates according to specifications such that the End Entity handles the out-of-band notification from the CA;
  - Interview appropriate personnel.

3.10.3.5 Certificate Distribution

This section covers the distribution of non-Root CA public keys.

Audit Procedures

Determine whether the requirements for certificate distribution, as stated in the applicable security-related documentation, are achieved. The auditor should consider performing the following procedures:

- Review certificate distribution documentation and ensure that certificates are distributed to relying parties in accordance with business requirements;
- Interview appropriate personnel.

3.10.3.6 Certificate Revocation

Audit Procedures

Ascertain the requirements for certificate revocation as stated in the applicable security-related documentation. The applicable security-related documentation should at least address the following:

- The applicable CA Certificate Policy and/or CPS specifies:
  - Who may request a certificate revocation;
  - Under what circumstances a certificate revocation request may be made;
  - Under what circumstances a certificate must be revoked.
- The RA authenticates the entity requesting revocation of a certificate;
- The RA verifies the authority of the entity requesting revocation of a certificate;
- The RA submits certificate revocation requests to the CA in an authenticated manner;
- The RA receives and verifies the confirmation that the CA has received the revocation request;
- The CA provides an authenticated acknowledgement of the revocation to the requesting entity;
- Certificate revocation requests are processed and validated in accordance with the requirements of the CPS;
- The CA updates the CRL upon certificate revocation;
- The CA provides an authenticated acknowledgement of the revocation to the entity whose certificate has been revoked.

Determine whether the requirements for certificate revocation, as stated in the applicable security-related documentation, are fulfilled. The auditor should consider performing the following procedures:

- Review documentation of the certificate revocation process;
- If revocation is allowed by individuals other than the subscriber, review documentation to ascertain whether notices of revocation are transmitted in an out-of-band fashion to the subscriber;
- Select a sample of revocations and ascertain whether an out-of-band communication occurred;

- Review documentation to gain an understanding of the event journals (audit trails) related to certificate revocations that are maintained;
- Test the accuracy of the event journals (audit trails) when testing the certificate revocation process;
- Select a sample of revocation requests and ascertain that the revocation request was properly validated prior to updating the certificate status and that the CRL or other status mechanism was updated appropriately;
- Reconcile the status of a selection of certificates within the repository to those in the CRL;
- Review documentation to determine whether only trusted personnel are allowed to perform certificate revocation functions;
- Review a sample of revocation transactions (e.g., revocation requests, including revocation/regeneration records) and assess the completeness and accuracy of certificate status records in the CA system;
- Review a sample of certificate revocations and determine whether a valid revocation/regeneration request has been received for certificates that have been revoked and/or regenerated;
- Interview appropriate personnel.

3.10.3.7 Certificate Suspension

Audit Procedures

Determine whether the requirements for certificate suspension, as stated in the applicable security-related documentation, are achieved. The auditor should consider performing the following procedures:

- Review documentation of the certificate suspension process and ensure it specifies who may request a suspension, under what circumstances a certificate suspension request may be made, and under what circumstances a certificate must be suspended;
- If suspension is allowed by individuals other than the subscriber, review documentation to ascertain whether notices of suspension are transmitted in an out-of-band fashion to the subscriber;
- Select a sample of suspensions and ascertain whether an out-of-band communication occurred;

- Review documentation to gain an understanding of the event journals (audit trails) that are maintained related to certificate revocations;
- Test the accuracy of the event journals (audit trails) when testing the certificate revocation process;
- Select a sample of suspension requests and ascertain whether the suspension request was properly validated prior to updating the certificate status, and that the CRL or other status mechanism was updated appropriately;
- Reconcile the status of a selection of certificates within the repository to those in the CRL;
- Review documentation to determine whether only trusted personnel are allowed to perform certificate suspension functions;
- Review a sample of suspension transactions (e.g., revocation requests) and assess the completeness and accuracy of certificate status records in the CA system;
- Review a sample of certificate revocations and determine whether a valid suspension request has been received for certificates that have been suspended;
- Review documentation that specifies under what circumstances a request may be made to lift a certificate suspension;
- Review a sample of requests to lift suspensions and ascertain whether they were properly validated;
- Interview appropriate personnel.

3.10.3.8 Certificate Revocation List (CRL) Processing

Audit Procedures

Determine whether the requirements for CRL processing, as stated in the applicable security-related documentation, are complied with. The auditor should consider performing the following procedures:

- Review documentation to gain an understanding of the process to generate CRLs and ensure that appropriate controls exist to ensure completeness of each generation of the CRL;
- Review documentation of the CA's CRL management process and perform the following procedures:

- Obtain documentation of the CRL management process and ensure only trusted personnel are allowed to perform CRL management functions;
- Review backup procedures for the archival of CRLs;
- Review personnel security policies and procedures related to the roles and responsibilities of trusted personnel.

- Review procedures to ensure that the CA makes the CRL available to the appropriate relying parties and evaluate for appropriateness;
- Review controls to ensure that a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. Test check through a sample of revoked certificates;
- Select a sample of days that a CRL was to be published, archived, and checked and ascertain that the CRL actions were performed in accordance with the policies within the CPS;
- Review the processes in place to identify when the distribution of a CRL to a relevant party fails;
- Review documentation to ascertain that the CRL has been digitally signed by the appropriate CA digital certificate prior to issuance;
- If required by the CPS or other service level agreements, review controls over the distribution of the CRLs to ensure timely and correct distribution to all relevant parties;
- Test the accuracy of the event journals (audit trails) when testing the CRL management process;
- Interview appropriate personnel.

3.11 INTRUSION DETECTION

Audit procedures and considerations

This section contains considerations for the IS auditor. Some of these considerations were covered in an operating system/server vulnerability or a firewall review. Where applicable, this is indicated for each consideration mentioned below. The IS auditor needs to ensure that these aspects were covered in the appropriate review. This can be done by evaluating the results of such review and evaluating the impact of negative findings on the risks in the intrusion detection area.

The implementation of the aspects mentioned below, will serve as preventative as well as detective controls for intrusion. The role of the IS auditor is to determine whether the following actions are performed by the organisation. (The areas impacted are also noted for each point, where applicable).

- Establish and maintain regular backup schedules and policies, particularly for important configuration information - *operating system and server vulnerabilities.*
- Establish and maintain appropriate password policies, especially access to highly privileged accounts - *operating system, server vulnerabilities, and access control*
- Implement properly designed firewalls - these can track all traffic in and out of the site, logging and inspecting every packet of information to ensure its legitimacy – *firewalls.*
- Keep all software up-to-date: implementing all security fixes and patches as they are released will go a long way to reducing vulnerability to these attacks. As available, install patches to guard against TCP SYN flooding – *firewalls and operating system.*
- Disable any unused or unneeded network services - *firewalls and operating system/ server vulnerabilities.*
- Enable quota systems on operating system if available i.e., limit users and programs to a certain amount of resources only – *operating system and server vulnerabilities*;
- If the operating system supports partitions or volumes, partition the file system so as to separate critical functions from other activities – *operating system and server vulnerabilities.*
- Establish system performance baselines and observe daily activity for aberrations - *server vulnerabilities.*
- Routinely examine the physical security environment with respect to current needs - *server vulnerabilities and physical security.*
- Use tools (e.g., Tripwire) to detect changes in configuration information or other files - *server vulnerabilities.*
- Invest in surplus and fault-tolerant network configurations.
- Switch on audit logs for all key servers: when efficiently and effectively configured and monitored, these logs will provide adequate information to identify and investigate any problems.

- Install intrusion detection software: if properly configured, this software will quickly identify known patterns of attack and immediately shut out only the attacker, while sounding the appropriate alarms.
- Hire the right people: make sure your technical personnel completely understand the issues, the technologies and the solutions.
- Test defenses regularly: the rapid rate of change in both the technology area and the hacking community means defenses must be tested on a regular basis.
- Design the network to isolate attacks: if the worst happens and the hacker gets inside, appropriate network configuration, firewalls and other tools will ensure any damage the hacker could cause is isolated to a small area – *firewalls*;
- Have an incident response plan: identifying, reacting to and resolving the problem immediately is the real business dilemma. Identify who should respond and test the plan. Establish procedures for determining the seriousness of the breach.
- Focus on preventative measures: swift, large volume, automated attacks require sophisticated, automated defense mechanisms. Identifying a problem an hour later and then trying to trace and resolve it is not an option.
- Gather evidence: understanding how to identify, gather and manage legal evidence to ensure the appropriate legal action can be taken against a hacker should be a key element of defense system design.
- Educate: constant awareness and updating of knowledge is the best defense to any attack - *server vulnerabilities.*
- Use network or file scanning tools to detect Distributed Denial of Service (DdoS) attacks and keep these up to date with new developments and types of attacks.
- Determine whether the system was designed to avoid allocating system resources for a potential user session before authentication is complete. Doing this would reduce denial of service attacks based on initiating many log-on attempts.
- Use a real-time system that can detect known attack signatures and patterns, as well as suspicious activity, including probes of the network or critical systems and unauthorized attempts to modify access control mechanisms. The system should be configurable to provide for immediate and automated alerts to such activity, and provide for configurable actions such as logging and automatically terminating the session.
- Immediate and tactful response is necessary in the event of a threat, attack, system compromise, or misuse of network resources. An Incident Response

Team should be formed and trained to respond to an identified security event. Automated response capabilities should be incorporated whenever possible.

- Tools for intrusion management therefore will include: use of monitoring software, the results of which are checked within a specific time-frame; automatic time-out; trend analysis; benchmarking; survey of markets for latest detection tools; patches and anti-virus software, as well as a system wide audit program.
- A system-wide audit program should be implemented to provide for immediate and full logging of activity to provide for user accountability. A central repository for the audit logs will provide immediate and historical reference in response to an investigation or management request for information. The program should also include security and statistical analysis tools to evaluate the audit logs. The audit program should include procedures to verify the integrity of individual systems and for compliance with existing system and security policies and procedures.

Determine whether the security requirements for incident response as stated in the applicable security-related documentation are achieved. The auditor should consider performing the following procedures:

- Review incident reporting and response policies and procedures;
- Review the incident categorisation/classification scheme;
- Review a sample of incident reports;
- Review a sample of reported incidents and determine whether incident response policies and procedures were followed;
- Interview personnel responsible for incident reporting and incident response;
- Review logs and reports of disciplinary measures taken;
- Interview personnel responsible for the disciplinary process.

APPENDIX B

GLOSSARY OF TERMS

The definitions of terms in this glossary are defined below in the context in which they were used in throughout this dissertation. These definitions were obtained from various Internet Online dictionaries and glossaries at the following Internet addresses:

http://whatis.com
http://www.onelook.com
http://www.pcwebopaedia.com
http://whatis.techtarget.com/
http://www.webopedia.com

Term	Definition
ANSI (X9)	*ANSI* (American National Standards Institute) is the primary organisation for fostering the development of technology standards in the United States. *ANSI* works with industry groups and is the U.S. member of the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from *ANSI* include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI). The X9 standard refers to standards for financial/banking.
Authentication	The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), *authentication* is commonly done through the use of log-on passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The action of verifying information such as identity, ownership, or authorisation.
Backbone	A *backbone* is a larger transmission line that carries data gathered from smaller lines that interconnect with it. 1) At the local level, a *backbone* is a line or set of lines that local area networks connect to for a wide area network connection or within a local area network to span distances efficiently (for example, between buildings). 2) On the Internet or other wide area network, a *backbone* is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network nodes.
Biometric authentication	A security measure for checking a network user's identity through the use of certain characteristics unique to the user such as a user's retina,

Bits	A *bit* (short for *binary digit*) is the smallest unit of data in a computer. A *bit* has a single binary value, either 0 or 1. Although computers usually provide instructions that can test and manipulate *bits*, they generally are designed to store data and execute instructions in *bit* multiples called bytes. In most computer systems, there are eight *bits* in a byte. The value of a *bit* is usually stored as either above or below a designated level of electrical charge in a single capacitor within a memory device.
Buffer overflow	A *buffer overflow* occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, *buffer overflow* is an increasingly common type of security attack on data integrity. In *buffer overflow* attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. *Buffer overflow* attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Certification authorities (CA)	A *CA* is a person or organisation that creates and manages issues around digital certificates.
Certificates	A *certificate* is an electronic document binding some pieces of information together such as a user's identity and public key – which is the key known to all in encryption and used to verify signatures.
Cgi-scripts	In computer programming, a *script* is a program or sequence of instructions that is interpreted or carried out by another program rather than by the computer processor (as a compiler program is). Some languages have been conceived expressly as *script* languages. In the context of the World Wide Web, Perl, VBScript, and similar *script* languages are often written to handle forms input or other services for a Web site and are processed on the Web server. In general, *script* languages are easier and faster to code in than the more structured and compiled languages such as C and C++ and are ideal for programs of very limited capability or that can reuse and tie together existing compiled programs. However, a *script* takes longer to run than a compiled program since each instruction is being handled by another program first (requiring additional instructions) rather than directly by the basic instruction processor.
Command processors	A program that accepts commands from the keyboard and causes the commands to be executed.
Console	(1) The combination of display monitor and keyboard (or other device that allows input). Another term for *console* is terminal. The term *console* usually refers to a terminal attached to a minicomputer or mainframe and used to monitor the status of the system. (2) Another term for monitor or display screen.

	(3) A bank of meters and lights indicating a computer's status, and switches that allow an operator to control the computer in some way.
Cookies	A *cookie* is information that a Web site puts on your har disk so that it can remember something about you at a later time. (More technically, it is information for future use that is stored by the server on the client side of a client/server communication.) Typically, a *cookie* records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A *cookie* is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the *cookies* that have been stored on your hard disk (although the content stored in each *cookie* may not make much sense to you). The location of the *cookies* depends on the browser. Internet Explorer stores each *cookie* as a separate file under a Windows subdirectory. Netscape stores all *cookies* in a single cookies.txt fle. Opera stores them in a single cookies.dat file. *Cookies* are commonly used to rotate the banner ads that a site sends so that it doesn't keep sending the same ad as it sends you a succession of requested pages. They can also be used to customise pages for you based on your browser type or other information you may have provided the Web site. Web users must agree to let *cookies* be saved for them, but, in general, it helps Web sites to serve users better.
Certificate Practice Statement	A *Certificate Practice Statement* (CPS) is a statement of the practices which a Certification authority employs in issuing and managing certificates.
Cryptographic module	Hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes or both.
Cryptograhic techniques	Techniques used to encrypt (cipher or code) a message in a way that the resulting coded message can be decrypted (deciphered or decoded) only by holders of the appropriate "key"
Deadly defaults	A deadly default is simply a pre-set configuration that is by default insecure.
Dial-up server	A *dial-up server* is a host computer on a network that answers requests for information from it. The server can be accessed by dialling up with a modem from a remote location. The term *server* is also used to refer to the software that makes the process of serving information possible.
Digital cash	Digital cash is an electronic payment system. It provides the consumer and merchant with a list of eligible banks with which to open electronic accounts – also a collection of bits recorded on a magnetic stripe.
Digital signatures	The electronic equivalent of traditional hand-written signatures. *Digital signatures* are performed in a more complex manner through the use of encryption.
Directory	A listing of directories (i.e., files that contains other files or directories).

listing	
Domain name	A *domain name* locates an organisation or other entity on the Internet. For example, the *domain name* : www.totalbaseball.com locates an Internet address for "totalbaseball.com" at Internet point 199.0.0.2 and a particular host server named "www". The "com" part of the *domain name* reflects the purpose of the organisation or entity (in this example, "commercial") and is called the top-level *domain name*. The "totalbaseball" part of the *domain name* defines the organisation or entity and together with the top-level is called the second-level *domain name.* The second-level *domain name* maps to and can be thought of as the "readable" version of the Internet address. A third level can be defined to identify a particular host server at the Internet address. In our example, "www" is the name of the server that handles Internet requests. (A second server might be called "www2".) A third level of *domain name* is not required. For example, the fully-qualified *domain name* could have been "totalbaseball.com" and the server assumed. Subdomain levels can be used. For example, you could have "www.nyyankees.totalbaseball.com". Together, "www.totalbaseball.com" constitutes a fully-qualified *domain name*. Second-level *domain names* must be unique on the Internet and registered with one of the ICANN-accredited registrars for the COM, NET, and ORG top-level domains. Where appropriate, a top-level *domain name* can be geographic. (Currently, most non-U.S. domain names use a top-level *domain name* based on the country the server is in.) To register a U. S. geographic *domain name* or a *domain name* under a country code, see an appropriate registrar. On the Web, the *domain name* is that part of the Uniform Resource Locator (URL) that tells a *domain name* server using the domain name system (DNS) whether and where to forward a request for a Web page. The *domain name* is mapped to an IP address (which represents a physical point on the Internet). More than one *domain name* can be mapped to the same Internet address. This allows multiple individuals, businesses, and organisations to have separate Internet identities while sharing the same Internet server. It may be worth noting that the *domain name* system contains an even higher level of domain than the top-level domain. The highest level is the root domain, which would be represented by a single dot (just as in many hierarchical file systems, a root directory is represented by a "/") if it were ever used. If the dot for the root domain were shown in the URL, it would be to the right of the top-level *domain name*. However, the dot is assumed to be there, but never shown.
Electronic bulletin boards	Provides a central clearing-house for information and correspondence about an almost infinite number of subjects. A shared file where users can enter information for other users to read or download. Many *bulletin boards* are set up according to general topics and are accessible throughout a network.
Electronic	An EC system where a Customer at a PC keys in information regarding

checks	a payment to a third party and signs the check with a digital signature.
Electronic currency	Electronic mathematical representation of money.
Electronic Data Interchange (EDI)	The electronic transfer of information from one organisation's application to another organisation's application using a standardised electronic form.
Electronic Funds Transfer (EFT)	The transfer of funds electronically by using magnetic tape, diskette, or systems designed for such purposes.
E-mail	A store and forward mail service that allows you to communicate throughout the network
Encryption	*Encryption* is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorised people. It relies upon cryptographic techniques.
Escrowed	A written agreement (or property or money) delivered to a third party or put in trust by one party to a contract to be returned after fulfillment of some condition
Extranet	The secured extensions of internal business processes to known external business partners using Internet derived applications and technology.
Fiber-optic cable	Cable that uses discrete light signals that are transmitted through a core of thin glass or plastic fibers.
Fingerprinting	When tracking the amount of traffic on a Web site, it refers to a person who visits a Web site more than once within a specified period of time. Software that tracks and counts Web site traffic can distinguish between visitors who only visit the site once and unique visitors who return to the site. Different from a site's hits or page views -- which are measured by the number of files that are requested from a site -- unique visitors are measured according to their unique IP addresses, which are like online *fingerprints*, and unique visitors are counted only once no matter how many times they visit the site. There are some ISPs that use Dynamic Host Configuration Protocol, such as AOL and cable modem providers, which use different IPs for every file requested, making one visitor look like many. In this case, a single IP address does not indicate a unique visitor. A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, *finger* only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a *finger* utility built into them.
FIPS 140-1	*FIPS* (Federal Information Processing Standards) are a set of standards that describe document processing, provide standard algorithms for

	searching, and provide other information processing standards for use within government agencies. *FIPS 140-1* defines the structure of cryptographic modules you must adhere to in computer and telecommunications systems. *FIPS 140-1* specifies security requirements that must be met by a cryptographic module used inside a security system that protects unclassified information that needs to be safeguarded during transmission and storage.
Firewall	A *firewall* is a set of related programs, located at a network server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Basically, a *firewall*, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A *firewall* also includes or works with a server that makes network requests on behalf of workstation users. A *firewall* is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.
Firmware	*Firmware* is programming that is inserted into programmable read-only memory (programmable ROM), thus becoming a permanent part of a computing device. *Firmware* is created and tested like software (using microcode simulation). When ready, it can be distributed like other software and, using a special user interface, installed in the programmable read-only memory by the user. *Firmware* is sometimes distributed for printers, modems, and other computer devices. IBM prefers the term microcode.
FTP	*File Transfer Protocol* (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, *FTP* is an application protocol that uses the Internet's TCP/IP protocols. *FTP* is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.
Hacker	*Hacker* is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems." Journalists or their editors almost universally use *hacker* to mean someone who attempts to break into computer systems. Typically, this kind of *hacker* would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.
Hacking	The art of seeking network and specific system access, promote levels of privileges in a target environment, and then use the promoted privilege to further expand access. Usually this access goes without

	authorisation.
HTTP	The *Hypertext Transfer Protocol (HTTP)* is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), *HTTP* is an application Protocol. Essential concepts that are part of *HTTP* include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an *HTTP* daemon, a program that is designed to wait for *HTTP* requests and handle them when they arrive. Your Web browser is an *HTTP* client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator) or clicking on a hypertext link, the browser builds an *HTTP* request and sends it to the Internet Protocol address indicated by the URL. The *HTTP* daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned.
HTML	*HTML (Hypertext Markup Language)* is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. Each individual markup code is referred to as an element (but many people also refer to it as a tag). Some elements come in pairs that indicate when some display effect is to begin and when it is to end. *HTML* is a formal Recommendation by the World Wide Web Consortium (W3C) and is generally adhered to by the major browsers, Microsoft's Internet Explorer and Netscape's Navigator, which also provide some additional non-standard codes
Internet	A global "network of networks" operating on a co-operative basis and owned by no one entity or organisation. The series of interconnected networks that include local area, regional, and national backbone networks. Networks in the *Internet* use the same telecommunications protocol (TCP/IP) and provide electronic mail, remote login, and file transfer services.
Interpreters	A command *interpreter* is the part of a computer operating system that understands and executes commands that are entered interactively by a human being or from a program. In some operating systems, the command *interpreter* is called the shell.
Intranet	A network connecting an affiliated set of clients using standard Internet protocols.
IP address	In the most widely installed level of the Internet Protocol (IP) today, an *IP address* is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your *IP address* in the message (actually, in each of the packets if more than one is required) and sends it to the *IP address* that is obtained by looking up the domain-name in the URL you requested or

in the e-mail address you're sending a note to. At the other end, the recipient can see the *IP address* of the Web page requestor or the e-mail sender and can respond by sending another message using the *IP address* it received.

An *IP address* has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the router that move packets from one point to another along the route - only the network part of the address is looked at.

The Network Part of the *IP Address*

The Internet Protocol (IP) is basically the set of rules for one network communicating with any other (or occasionally, for broadcast messages, all other networks). Each network must know its own address on the Internet and that of any other networks with which it communicates. To be part of the Internet, an organisation needs an Internet network number, which it can request from the Network Information Center (NIC). This unique network number is included in any packet sent out of the network onto the Internet.

The Local or Host Part of the *IP Address*

In addition to the network address or number, information is needed about which specific machine or host in a network is sending or receiving a message. So the *IP address* needs both the unique network number and a host number (which is unique within the network). (The host number is sometimes called a local or machine address.)

Part of the local address can identify a subnetwork or subnet address, which makes it easier for a network that is divided into several physical subnetworks (for example, several different local area networks) to handle many devices.

IP Address Classes and Their Formats

Since networks vary in size, there are four different address formats or classes to consider when applying to NIC for a network number:

Class A addresses are for large networks with many devices.

Class B addresses are for medium-sized networks.

Class C addresses are for small networks (fewer than 256 devices).

Class D addresses are multicast addresses.

The first few bits of each *IP address* indicate which of the address class formats it is using. The address structures look like this:

The *IP address* is usually expressed as four decimal numbers, each representing eight bits, separated by periods. This is sometimes known as the dot address and, more technically, as dotted quad notation. For Class A *IP addresses*, the numbers would represent "network.local.local.local"; for a Class C *IP address*, they would represent "network.network.network.local". The number version of the IP address can (and usually is) represented by a name or series of names called the domain name.

The Internet's explosive growth makes it likely that, without some new architecture, the number of possible network addresses using the scheme above would soon be used up (at least, for Class C network addresses). However, a new IP version, IPv6, expands the size of the *IP address* to 128 bits, which will accommodate a large growth in the number of network addresses. For hosts still using IPv4, the use of subnets in the host or local part of the IP address will help reduce new applications for network numbers. In addition, most sites on today's mostly IPv4 Internet have gotten around the Class C network address

	limitation by using the Classless Inter-Domain Routing (CIDR) scheme for address notation. Relationship of the *IP Address* to the Physical Address The machine or physical address used within an organisation's local area networks may be different than the Internet's *IP address.* The most typical example is the 48-bit Ethernet address. TCP/IP includes a facility called the Address Resolution Protocol (ARP) that lets the administrator create a table that maps IP addresses to physical addresses. The table is known as the ARP cache. Static versus Dynamic *IP Addresses* The discussion above assumes that *IP addresses* are assigned on a static basis. In fact, many IP addresses are assigned dynamically from a pool. Many corporate networks and online services economise on the number of IP addresses they use by sharing a pool of *IP addresses* among a large number of users. If you're an America Online user, for example, your *IP address* will vary from one logon session to the next because AOL is assigning it to you from a pool that is much smaller than AOL's base of subscribers.
ISO	*ISO* (International Organisation for Standardisation), founded in 1947, is a worldwide federation of national standards bodies from some 100 countries, one from each country. Among the standards it fosters is Open Systems Interconnection (OSI), a universal reference model for communication protocols. Many countries have national standards organisations such as the American National Standards Institute (ANSI) that participate in and contribute to *ISO* standards making. "ISO" is not an abbreviation. It is a word, derived from the Greek *isos*, meaning "equal", which is the root for the prefix "iso-" that occurs in a host of terms, such as "isometric" (of equal measure or dimensions) and "isonomy" (equality of laws, or of people before the law). The name *ISO* is used around the world to denote the organisation, thus avoiding the assortment of abbreviations that would result from the translation of "International Organisation for Standardisation" into the different national languages of members. Whatever the country, the short form of the Organisation's name is always *ISO.*
Java-Beans	Enterprise *JavaBeans (EJB)* is a Java Application Program Interface developed by Sun Microsystems that defines a component architecture for multi-tier client/server systems. *EJB* systems allow developers to focus on the actual business architecture of the model, rather than worry about endless amounts of programming and coding needed to connect all the working parts. This task is left to *EJB* server vendors. Developers just design (or purchase) the needed *EJB* components and arrange them on the server. Because *EJB* systems are written in Java, they are platform independent. Being object oriented, they can be implemented into existed systems with little or no recompiling and configuring.
Key Escrow	If you store data in an encrypted fashion and lose the digital encryption key, you probably have no way of ever reading that data again unless somebody else happens to be holding the key for you (*key escrow*).
Modem	A device for translating the digital data of computers into analogue signals. Two or more computers connected together over phone lines

	are therefore able to exchange files, and generally communicate with each other.
Network	A collection of two or more interconnected computers, for the purpose of sharing and transferring data via telecommunications.
Node	In a network, a *node* is a connection point, either a redistribution point or an end point for data transmissions. In general, a *node* has programmed or engineered capability to recognize and process or forward transmissions to other nodes
Operating System	An *operating system* (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications.
OSI ISO	*OSI (Open Systems Interconnection)* is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although *OSI* is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the *OSI* model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion. *OSI* was officially adopted as an international standard by the International Organisation of Standards (ISO).
Out of bound	*Out of band* implies the use of methods independent of the primary communications means e.g. *out of band* signaling is telecommunication signaling (exchange of information in order to control a telephone call) that is done on a channel that is dedicated for the purpose and separate from the channels used for the telephone call.
Packet Sniffer	A tool that can capture conversations between two or more systems or devices. It captures network traffic and decodes (interprets) it.
Patches	A *patch* (sometimes called a "fix") is a quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems (called bug) will almost invariably be found. A *patch* is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's Web site. The *patch* is not necessarily the best solution for the problem and the product developers often find a better solution to provide when they package the product for its next release. A *patch* is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of *patches*.
Portal/ Gateway	*Portal* is a new term for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or

	that users tend to visit as an anchor site. There are general portals and specialized or niche portals. Some major general portals include Yahoo, Excite, Netscape, Lycos, CNET, Microsoft Network, and America Online's AOL.com. Examples of niche portals include Garden.com (for gardeners), Fool.com (for investors), and SearchNT.com (for Windows NT administrators). Typical services offered by portal sites include a directory of Web sites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum.
Protocol	A *Protocol* is a set of rules that defines how computers transmit information to each other, which allows different types of computer and software programs to communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard.
Registration Authority (RA)	A *registration authority* (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. *RA*s are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.
Random number generator (RNG)	A pseudo-*random number generator* (PRNG) is a program written for, and used in, probability and statistics applications when large quantities of random digits are needed. Most of these programs produce endless strings of single-digit numbers, usually in base 10, known as the decimal system. When large samples of pseudo-random numbers are taken, each of the 10 digits in the set {0,1,2,3,4,5,6,7,8,9} occurs with equal frequency, even though they are not evenly distributed in the sequence. Many algorithms have been developed in an attempt to produce truly random sequences of numbers, endless strings of digits in which it is theoretically impossible to predict the next digit in the sequence based on the digits up to a given point. But the very existence of the algorithm, no matter how sophisticated, means that the next digit can be predicted. This has given rise to the term pseudo-random for such machine-generated strings of digits. They are equivalent to random-number sequences for most applications, but they are not truly random according to the rigorous definition. The digits in the decimal expansions of irrational numbers such as pi (the ratio of a circle's circumference to its diameter in a Euclidean plane), *e* (the natural-logarithm base), or the square roots of numbers that are not perfect squares (such as $2^{1/2}$ or $10^{1/2}$) are believed by some mathematicians to be truly random. But computers can be programmed to expand such numbers to thousands, millions, billions, or trillions of decimal places; sequences can be selected that begin with digits far to the right of the decimal (radix) point, or that use every second, third, fourth, or *n*th digit. However, again, the existence of an algorithm to determine the digits in such numbers is used by some theoreticians to argue that even these single-digit number sequences are pseudo-random, and not truly random. The question then becomes, Is the

	algorithm accurate (that is, random) to infinity, or not? - and because no one can answer such a question definitively because it is impossible to travel to infinity and find out, the matter becomes philosophical.
Routers	On the Internet, a *router* is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The *router* is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A *router* is located at any gateway (where one network meets another), including each Internet point-of-presence. A *router* is often included as part of a network switch.
Router tables	A router table is used by routers to determine the address of the next device in the communication path.
Server	1) In general, a *server* is a computer program that provides services to other computer programs in the same or other computers. 2) The computer that a *server* program runs in is also frequently referred to as a server (though it may contain a number of server and client programs). 3) In the client/*server* programming model, a *server* is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a *server* of requests from other programs.
Smart Card	A *smart card* is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use. A *smart card* contains more information than a magnetic stripe card and it can be programmed for different applications. Some cards can contain programming and data to support multiple applications and some can be updated to add new applications after they are issued. *Smart cards* can be designed to be inserted into a slot and read by a special reader or to be read at a distance, such as at a toll booth. Cards can be disposable (as at a trade-show) or reloadable (for most applications).
SMTP traffic	*SMTP (Simple Mail Transfer Protocol)* is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses *SMTP* for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server. Most mail programs such as Eudora let you specify both an *SMTP* server and a POP server. On UNIX-based systems, sendmail is the most widely-used *SMTP* server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for Windows NT.
Sniffer	A *sniffer* is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Using this information, a network manager can keep traffic flowing efficiently.

	A *sniffer* can also be used legitimately or illegitimately to capture data being transmitted on a network. A network router reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or whether it should be passed further along the Internet. A router with a *sniffer*, however, may be able to read the data in the packet as well as the source and destination addresses. *Sniffers* are often used on academic networks to prevent traffic bottlenecks caused by file-sharing applications such as Napster or Gnutella.
Spoofing	On the Internet, "to *spoof*" can mean: 1) To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user) 2) To simulate a communications protocol by a program that is interjected into a normal sequence of processes for the purpose of adding some useful function 3) To playfully satirise a Web site.
Subnets	A *subnet* (short for "subnetwork") is an identifiably separate part of an organisation's network. Typically, a *subnet* may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organisation's network divided into *subnets* allows it to be connected to the Internet with a single shared network address. Without *subnets*, an organisation could get multiple connections to the Internet, one for each of its physically separate subnetworks, but this would require an unnecessary use of the limited number of network numbers the Internet has to assign. It would also require that Internet routing tables on gateways outside the organisation would need to know about and have to manage routing that could and should be handled within an organisation.
Switches	In telecommunications, a *switch* is a network device that selects a path or circuit for sending a unit of data to its next destination. A *switch* may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a *switch* is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.
Tamper evident envelopes	Tamper evident security envelopes are an excellent way to ensure that valuable documents or objects remain safe when mailed The security envelopes are sealed with tamper evident tape that shows a "VOID/OPENED" message when peeled away, clearly showing the recipient that the contents have more than likely been tampered with if the message is showing. These tamper evident security envelopes are preprinted with consecutive numbers, address, and return address lines, and a numbered receipt, so using these security envelopes to protect your mailings is a simple process. When sending valuable documents or personal belongings via mail or courier, a durable security envelope that incorporates a theft deterrent like a tamper evident tape, is the best choice. If the tamper evident

	security envelope arrives with the words "VOIDS/OPENED" showing on the face of the tape, the recipient need only refuse the shipment. In this way, you can be sure that the recipient will not be receiving an empty envelope or an envelope filled with worthless materials.
Two factor authentication	*Two-factor authentication* is a security process that confirms user identities using two distinctive factors – something you know, such as a Personal Identification Number (PIN), and something you have, such as a smart card or token.
TCP/IP	*TCP/IP (Transmission Control Protocol/Internet Protocol)* is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the *TCP/IP* program just as every other computer that you may send messages to or get information from also has a copy of *TCP/IP*. *TCP/IP* is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.
Telnet	A terminal emulation program for TCP/IP networks such as the Internet. The *Telnet* program runs on your computer and connects your PC to a server on the network. You can then enter commands through the *Telnet* program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a *Telnet* session, you must log in to a server by entering a valid username and password. *Telnet* is a common way to remotely control Web servers.
Time stamping	A record mathematically linking a document to a time and date.
URL	*Universal Resource Locator* - (URL) An address that identifies the location of any type of Internet resource.
VAN (value added network)	A private network provider (sometimes called a turnkey communications line) that is hired by a company to facilitate electronic data interchange (EDI) or provides other network services. Before the arrival of the World Wide Web, some companies hired *value-added networks* to move data from their company to other companies. With the arrival of the World Wide Web, many companies found it more cost-efficient to move their data over the Internet instead of paying the minimum monthly fees and per-character charges found in typical *VAN* contracts.
Virtual private network (VPN)	A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A *virtual private network* can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the *VPN* is to give the company the same

	capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A *virtual private network* makes it possible to have the same secure sharing of public resources for data. Using a *virtual private network* involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.
Web browser	A program, which sends requests for information across the Internet and displays the information when it is received and uses a graphical approach to finding and displaying the information on the Internet.
Web server	A *Web server* is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a *Web server* program. Two leading *Web servers* are Apache, the most widely-installed Web server, and Microsoft's Internet Information Server (IIS). Other *Web servers* include Novell's *Web Server* for users of its NetWare operating system and IBM's family of Lotus Domino servers, primarily for IBM's OS/390 and AS/400 customers. *Web servers* often come as part of a larger package of Internet- and intranet-related programs for serving e-mail, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages. Considerations in choosing a *Web server* include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and publishing, search engine, and site building tools that may come with it.
Web-wrap	A Web Wrap agreement sets forth contractual terms in an on-line environment and is a form of Standard Form Agreement since one party drafts the terms of the agreement without consultation or negotiation of such terms with the other party or parties. A web wrap agreement usually appears as a dialogue box on a customer's screen when the customer attempts to download software or order goods or services on-line. The dialogue box contains the terms and conditions of the license or sale which the customer is instructed to review before assenting thereto by clicking a button at the bottom of the dialogue box.
World wide Web (WWW)	A graphical environment that provides easy access to information stored on systems connected to the Internet. The *WWW* allows users to retrieve software and text on to their own computers for future use.
X.509	The most widely used standard for defining digital certificates. *X.509* is actually an International Telecommunications Union (ITU) Recommendation, which means that has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use *X.509* certificates to implement SSL in their Web servers and browsers. But an *X.509* Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

REFERENCES

A

Agrireview October 1998, Available on Internet: http://www.Agrireview/october98/agrfeat3.htm: page 1 and 2. Date visited: 12 October 1998.

AARF. 2000. Electronic Commerce: Audit Risk Assessments and Control Considerations, AGS 1056. Australian Accounting Research Foundation, Melbourne.

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B. 1998. 'The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption. [Online]. Available at Internet: http://www.cdt.org/crypto/risks98/. Date visited: 12 October 2001.

Abrema. 2002. Glossary of Auditing Terms. [Online]. Available at Internet: http://www.abrema.net/abrema/audit_approach_g.html. Date visited: 5 February 2002.

Accountants World. 2002. Big 5 Firms (5). [Online]. Available at Internet: http://www.accountantsworld.com/miscresources.asp?linktype=special&cat=Big+5+firms Date visited: 11 June 2002.

AICPA. 1997. AICPA Professional Standards – Responsibilities and Functions of the Independent Auditor (AU110). American Institute of Certified Public Accountants Inc. New York, USA.

AICPA, 1997. AICPA Professional Standards. American Institute of Certified Public Accountants Inc. New York, USA.

AICPA2. 1997. AICPA Professional Standards – Auditing in a Computer Systems Environment (AU8401). American Institute of Certified Public Accountants Inc. New York, USA.

AICPA3. 1997. AICPA Professional Standards. American Institute of Certified Public Accountants Inc. New York, USA.

AICPA. 1998. WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce. version 1.0. 1997. [Online]. Available at Internet: http://www.aicpa.org. Date visited: 21 August 1999.

AICPA1. 1998 Top 10 Technology Issues. [Online]. Available at Internet: http://www.aicpa.org. Date visited: 23 August 1999.

AICPA. 1999. WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce. Version 2.0 October 15 1999. [Online]. Available at Internet: http://www.aicpa.org. Date visited: 21 August 2000.

Ams. 2001. Internal Control Guide for Managers. [Online]. Available at Internet: http://www.ams.vt.edu/control.html. Date visited: 21 September 2001

Andersen. 2002. Audit and Assurance Services. [Online]. Available at Internet: http://www.andersen.com/website.nsf/content/EuropeIrelandIndustry9!OpenDocument. Date visited: 8 February 2002.

Apacheweek. 2000. Using Certificate Revocation Lists. [Online]. Available at Internet: http://www.apacheweek.com/features/crl. Date visited: 6 November 2001.

Asokan, N. Phillipe A. Steiner, J.M., Waidner, M. 1997. The State of the Art in Electronic Payment Systems. [Online]. Available at Internet: http://www.ibm.com. Date visited: 27 June 2001.

Audit Commission. 2000. Who Audits the Auditors? [Online]. Available at Internet: http://www.audit-commission.gov.uk/publications/general.shtml. Date visited: 12 January 2001.

B

Baltimore. 1999. An Introduction to Public Key Infrastructure. [Online]. Available at Internet: http://www.baltimore.com. Date visited: 24 March 1999.

Baltimore. 1999. Global E-security. [Online]. Available at Internet: http://www.baltimore.com. Date visited: 27 April 2000.

BC. 2001. Internal Control definitions. [Online]. Available at Internet: http://www.bc.edu/bc_org/fvp/ia/ic/def.html. Date visited: 21 September 2001.

Beck, D.F. 2001. A Review of Cybersecurity Risk Factors. [Online]. Available at Internet: http://www/sans.org/infosecFAQ/securitybasics/risk.htm. Date visited: 27 July 2001.

Berbera, J. & Karasniak, P. & Pak, M. 1997. Security in E-Commerce. [Online]. Available at Internet: http://www.stern.nyu.edu/~prk204/combilpaper.htm. Date visited: 04 July 2001.

Blunt. J. 1997. Internet Security: An Oxymoron. [Online]. Available at Internet: http://www.decus.org/decus/pubs/magazine. Date visited: 26 June 1998.

Bohm, N., Brown, I., Gladman, B. 2000. Maintaining Consumer Confidence in Electronic Payment Mechanisms. [Online]. Available at Internet: http://elj.warwick.ac.uk/jilt/00-3/. Date visited: 22 February 2001.

Bradley. 2002. Type of Auditor. [Online]. Available at Internet: http://bradley.edu/~simonp/atg457/chapter01.doc. Date visited: 04 June 2002.

Business Majors. 2002. Major Accounting Firms. Available at Internet: http://businessmajors.about.com/cs/accountingfirms. Date visited: 11 June 2002.

C

CERT. 1999. Practices about Hardening and Securing Systems. [Online]. Available at Internet: http://www.cert.org/security-improvement/#harden. Date visited: 15 October 2001.

Certicom. 1997. Elliptic Curve Cryptosystem. [Online], Available at Internet: http://www.certicom.com. Date visited: 27 June 2000.

Choi, S. & Stahl, D.O. & Whinston, A.B. 1999. Payments and the Future of Electronic Commerce. The University of Texas at Austin. [Online]. Available at Internet: http://www.uts.cc.utexas.edu/soon/vita/cyberpayments.html. Date visited: 25 March 2000.

CICA. 1986. Computer Control Guidelines. The Canadian Institute of Chartered Accountants.

CISA. 2001. 2001 CISA Review Technical Information Manual. Information Systems Audit and Control Association. pp 20, 24, 25, 30.

Cknow. 2000. Denial of Service. [Online]. Available at Internet: http://www.cknow.com/ckinfo/def_d/denialofservice.shtml. Date visited: 7 November 2001.

Cobb, S. 1998. Security Issues in Internet Commerce - ICSA White Paper on Internet Commerce Version 2.0. [Online]. Available at Internet: http://www.2cobbs.com/news. Date visited: 15 April 2000.

Companies-house. 2000. Auditors. [Online]. Available at Internet: http://www.companies-house.gov.uk/notes/gba4.html. Date visited: 4 December 2001.

Cooper, V.R.V. 1982. Student's Manual of Auditing. Second Edition. Gee & Co (Publishers) Limited, United Kingdom. pp 3, 28-30.

Concord. 2000. E-Business Survival Guide. [Online]. Available at Internet: http://concord.com/resctr/survival/survival.htm. Date visited: 8 February 2001.

Cott, D. 2001. Enterprise Security Management - It's In Your Hands. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

CPG. 1999. SSL – 1, SET – 0. [Online]. Available at Internet: http://webserver.cpg.com/news/4.7/n2.shtml. Date visited: 5 November 2001.

CPGCA. 2001. Auditing. [Online]. Available at Internet: http://www.cpgca.co.za/auditing.htm. Date visited: 7 February 2002.

CSE. 2001. Network Security and Cryptography. [Online]. Available at Internet: http://www.cse.ucsd.edu/Research/security.html. Date visited: 6 November 2001.

CSU (Colorado State University). 2002. Colorado State University Libraries Business Details. [Online]. Available at internet: http://patriot.library.colostate.edu/research/business/resourceDetail.php?resourceID=19. Date visited: 11 June 2002.

D

Dallas, D.A. 1998. Electronic Commerce Security on the Internet. Auerbach Publications 74-15-01. CRC Press LLC.

de Beaupré, A. 2001. Know yourself: Vulnerability Assessments. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

Dekker, M. 1997. Security of the Internet. [Online]. Available at Internet: http://www.cert.org/encyc_article/tocencyc.html. Date visited 7 November 2001.

Deloitte. 2001. Our Audit Approach and Technology. [Online]. Available at Internet: http://www.deloitte.com.ky/assuranceapproach.htm. Date visited: 5 February 2002.

Deloitte & Touche. 1997. Taking the Mystery out of Firewalls. [Online]. Available at Internet: http://www.dttus.com/risk/info/pubs/mystery. Date visited: 6 January 1999.

Denny S. 1997. The Electronic Commerce Challenge. [Online]. Available at Internet: http://www.denny.dc3.com. Date visited: 18 January 1999.

Dfat. 2000. Electronic Commerce – An Australian Customs Perspective. [Online]. Available at Internet: http://www.dfat.gov.au/apec/ecom/custec1.html. Date visited: 25 June 2001.

Dixon, K.L. 1999. Electronic Commerce Security. [Online]. Available at Internet: http://www.aph.gov.au/library/pubs/rp/1998-99/99rp12.htm. Date visited: 19 June 2001.

Duncan, D. 1996. An Emerging Tool for Today's Marketplace: Electronic Commerce. *IS Audit &Control journal*, Volume VI 1996: 6-7.

Duques, R & Staglin, G.K. 2000. E-Commerce Whitepaper. [Online]. Available at Internet: http://www.eoneglobal.com/whtpaper.html. Date visited 25 June 2001.

E

ECA. 1999/2000. What is e-commerce?. [Online]. Available at Internet: http://www.eca.org.uk/products_businesstech_payments.asp. Date visited: 14 July 1999.

Ecommerceabout, 2001. E-commerce primer. [Online]. Available at Internet: http://www.ecommerceabout.com. Date visited: 6 May 2001.

Ecommerce-merchant-accounts. 1999. Ecommerce history. [Online]. Available at Internet: http://www.ecommerce-merchant-accounts.com/. Date visited: 29 June 2001.

EDPAA. 1983. Auditing Information Systems A Step-by-Step Approach. EDO Auditors Foundation, IL. USA.

EDP Auditors Foundation (now ISACA). 1994. General Standards for Information Systems Auditing. *IS Audit & Control Journal*, Volume I, 1994: 60.

EIU. 2002. Big 5 CPA Firms. [Online]. Available at internet: http://www.eiu.edu/~ldudley/big5.htm. Date visited: 11 June 2002.

Elliott, R. & Pallais, D. M. 1997. Are you Ready for Assurance Services? *AICPA Journal of Accounting,* June 1997: 47-51.

EM, 1993. Electronic Markets, No 9 to 10 October 1993. University of St Gallen, Institute for Information Management. Page1.

Emich (Eastern Michigan University). 2002. Worldwide Fee Income of the Big Five. [Online]. Available at Internet: http://www.emich.edu/public/accounting/big5.htm. Date visited: 11June 2002.

Emory. 2000. Emory University Internal Audit. [Online]. Available at Internet: http://www.emory.edu/IAD/. Date visited: 1 December 2001.

Entrust. 1998. Computer security fact sheet. [Online]. Available on Internet: http://www.entrust .com. Date visited: 21 March 1999.

European Commission. 2000. Electronic Commerce – An Introduction. [Online]. Available at Internet: http://europaeuint/ISPO/ecommerce/answers. Date visited: 29 June 2001.

E-witness. 2001. Security FAQs. [Online]. Available at Internet: http://www.e-witness.ca/faq.phtml. Date visited: 2 November 2001.

EY. 2002. Focused Approach. [Online]. Available at Internet: http://www.ey.com/GLOBAL/gcr.ncf/Isle_of_Man/Audit_&_Assurance_Approach. Date visited: 5 February 2002.

F

FDIC. 1999. Security Risks Associated With The Internet. [Online]. Available at Internet: http://www.spicersweb.net/fdic.htm. Date visited: 12 October 2001.

Feindt, S. & Culpin, I. 1998. Electronic Commerce and Secure Telecommunications. [Online]. Available at Internet: http://www.europa.eu.int/Informationsecurity/ecommerce. Date visited: 15 June 2001.

Feinman, T., Goldman, D., Wong, R., Cooper, N. 1999. Security Basics: A White Paper. [Online]. Available at Internet: http://www.itaudit.org/forum/security. Date visited: 31 July 2001.

Flanagan, T. & Safdie, E. 1997. Internet Security Primer. [Online]. Available at Internet: http://www.techguide.com. Date visited: 28 October 2000.

Fratto, M. 2000. Certificate Revocation: When Not To Trust. [Online]. Available at Internet: http://www.nwc.com/1112/1112ws1.html. Date visited: 15 November 2001.

Fuller, E.R. 2000. Denial of Service Attack. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

G

Gallegos, F. & Bieber, D.W. 1987. Emerging Technology and Information Systems Auditing. EDP Auditing Article number 71-01-10. Auerbach Publishers Inc.

Garceau, L., Matos, V., Misra, S.K. 1998. 'The use of electronic money in electronic commerce transactions'. *IS Audit &Control Journal, Vol III*, 1998, Published by the Information Systems Audit & Control Association. pp14 – 24.

Garfinkel, S. & Spafford, G. 1997. Web security & Commerce. O'Reilly & Associates Inc: First Edition, June 1997. USA.

Garitte, J. P. 1998. Keeping exec mgmt focus on IT part I. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

GASSP. 1997. Generally Accepted System Security Principles. [Online]. Available at Internet: http://web.mit.edu/security/www/gassp1.html. Date visited: 28 August 2001.

Genuity. 1998. GTE to Offer one-stop validation for Digital Certificates. [Online]. Available at Internet: http://www.genuity.com/announcements/news/press_release_19981217-01.xml. Date visited: 6 November 2001.

Ghosh, A.K. 1997. E-commerce Security. John Wiley & Sons, USA.

Ghosh, A. K. 1999. Securing E-Commerce: A Systematic Approach. [Online]. Available at Internet: http://www.rstcorp.com/~anup aghosh@rstcorp.com. Date visited: 18 January 1999.

Ghostship. 2001. Denial of Service Attack. [Online]. Available at Internet http://www.ghostship.com. Date visited: 18 October 2001.

Gilhooley, I.A. 1990. The EDP Internal/External Auditor Relationship. EDP Auditing Article number 72-01-60. Auerbach Publishers Inc.

Globalsign. 1999. Globalsign to Offer ValiCert Services and Products to its Clients in Europe. [Online]. Available at Internet: http://www.globalsign.net/company/press/valicert.htm. Date visited: 6 November 2001.

Gregg, S. 2000. A Response to Recent Cyber Attacks. [Online]. Available at Internet http:www.isaca.org. Date visited: 25 July 2000.

GT. 2000. The Internal Audit Role in Singapore Listed Companies. [Online]. Available at Internet: http://www.gt.com.sg/art_ia.doc. Date visited: 2 December 2001.

H

Halsey, B. 1996. Certification Authority Frequently Asked Questions (CA-FAQ). [Online]. Available at Internet: http://www.anl.gov/ECT/certify/CA-FAQ.html. Date visited: 3 November 2001.

Hartman, S. 2001. Securing E-Commerce: An Overview of Defense In-depth. [Online]. Available at Internet: http://www/sans.org/infosecFAQ/start/sec_ecom.htm. Date visited: 27 July 2001.

Held, G. 1994. Securing electronic messages. EDP Auditing - Auerbach Publications, Warren Gorham & Lamont. p5.

Held, G. 1997. Electronic Commerce. EDP Auditing - Auerbach Publications. p7.

Hickman, J.R. 1996. Practical IT Auditing. Warren, Gorham & Lamont A1.04.

Hinton, C. 2000. Managing your e-Business Environment. [Online]. Available at Internet: http://www.heroix.com. Date visited: 11 December 2000.

Hunton, J. E. & Holstrum, G. 1998. The Role of Information Systems Auditors in WebTrust Assurance. *IS Audit & Control Journal*, Volume III, 1998 pp.39-43.

I

IAPC (International Auditing Practices Committee). 2001. Electronic Commerce Using the Internet or Other Public Networks. IAPC.

iBig5. 2002. The Global Website for Alumni of the Big 5 Accounting Firms. [Online]. Available at Internet: http://www.ibig5.com/structure.cfm. Date visited: 11 June 2002.

IC (Imperial College of Science Technology, and Medicine). 2000. Internal Audit. [Online]. Available at Internet: http://www.ad.ic.ac.uk/int_audit/intaudit.htm. Date visited: 2 January 2002.

ICAS - The Institute of Chartered Accountants in Scotland. 1998. [Online]. Discussion paper on Electronic Commerce. Available at Internet: http://www.icas.org.uk/members/servicesfrom. Date visited: 14 July 1999.

IEC. 2000. Internet Security. [Online]. Available at Internet: http://www.iec.org/online/tutorials/int_sec/index.html. Date visited: 25 July 2001.

IFAC. 1998. Managing Security of Information. [Online]. Available at Internet: http://www.theiia.org/ecm/guide-ia.cfm?doc_id849. Date visited: 24 October 2001.

Interhack. 1997. Introduction to Network Security. [Online]. Available at Internet: http://www.interhack.net/pubs. Date visited: 2 November 2001.

Internalaudit. 2001. Our Typical Work Plan Approach. [Online]. Available at Internet: http://www.internalaudit.co.uk/work.html. Date visited: 12 February 2002.

Irving L. 1998. The Risks and Rewards of Electronic Commerce (Information technology expands business). [Online]. Available at Internet: http://www.usembassy-israel.org/il/publish/press/trade/archive/1997/October/et11009.htm. Date visited: 25 June 1998.

ISACA. 1999. Control Objectives for Information and Related Technology (COBIT) Framework – Executive Overview. Published by the Information Systems Audit and Control Association.

ISACA. 2000. E-commerce Security: Enterprise Best Practices. [Online]. Available at Internet: http://www.isaca.org/ecomm-e2.htm. Date visited: 13 September 2000.

ISACA. 2001. 2001 CISA Review Technical Information Manual. Information Systems Audit and Control Association. pp 20, 25, 30.

ISACA1. 2001. Standards for Information Systems Auditing. [Online]. Available at Internet: http://www.isaca.org/standard/en.htm. Date visited: 15 October 2001.

IUSB. 2002. Audit Function in Society. [Online]. Available at Internet: http://iusb.edu/~respahbo/audit01.ppt. Date visited: 04 June 2002.

J

James, M.L. 1999. Electronic Commerce: Security Issues. [Online]. Available at Internet: http://www.aph.gov.au/library/pubs/rp/1998-99/99rp12.htm. Date visited: 17 July 2001.

Jones, C. 2001. Internet Security Software: The Ultimate Internet Infrastructure. [Online]. Available at Internet: http://www.itaudit.org/forum/internet. Date visited: 28 October 2001.

K

Kabay, M.E. 1998. Identification, Authentication and Authorization on the World Wide Web. [Online]. Available at Internet: http:www.icsa.org/knet. Date visited: 03 February 2000.

Kessler, G.C. 2000. Defenses Against Distributed Denial of Service Attacks. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/threatsDDoS.htm. Date visited: 5 November 2001.

KPMG. 1995. KPMG TTP services methodology. published by KPMG, Netherlands.

KPMG. 1998. Secure Commerce in the Information Age. KPMG International Headquarters. Page 12.

KPMG. 2000. Our Audit Approach. [Online]. Available at Internet: http://www.kpmg.ie/audit/approach.htm. Date visited: 5 February 2002.

KPMG. 2002. Assisting Internal Audit. [Online]. Available at Internet: http://ourworld.compuserve.com/homepages/BIverson/irm-ia.htm. Date visited: 15 February 2002.

L

La Macchia, B.A. 2001. Certificate Revocation Mechanics. [Online]. Available at Internet: http://www.farcaster.com/papers/fc98/html/node3.html. Date visited: 5 November 2001.

Landrum, D.E. 2001. Web Application and Databases Security. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

LeClerc, R. 2001. Audit and Security Control Issues when Conducting Information Security Reviews. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 28 July 2001.

Le Tocq, C. & Young, S. 1998. SET Comparative Performance Analysis - A White Paper from GartnerGroup. [Online]. Available at Internet: http:www.epaynews.com/links/set.html. Date visited: 4 August 2000.

Levi, A. & Koc, C.K. 2001. Reducing Certificate Revocation Cost using NPKI. Available at Internet: http://citeseer.nj.nec.com/441154.html. Date visited: 26 October 2001.

Levy, E. 2000. DDoS Attack Mitigation. [Online]. Available at Internet: http://security.royans.net/info/posts/bugtraq_ddos.shtml. Date visited: 31 October 2001.

Liang, E.P. 1999. Future Trend of Electronic Commerce. [Online]. Available at Internet: http://signet.com.sg. Date visited: 12 June 2000.

Lindner, C.E. 2001. Information Security Primer. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

Lymer, A. 2000. AuSSB Release Worlds Most Developed Guide on Ecommerce Audits' [Online]. Available at Internet: http://www.aarf.asn.au. Date visited: 15 September 2000.

M

Mackey, R. & Gossels, J. 2000. Mastering Fundamentals, Part 1. [Online]. Available at Internet: http://www.infosecuritymag.com/articles/january00/features3.shtml. Date visited: 21 August 2001.

Mahadevan, C. 2001. Intrusion, Attack, Penetration – Some Issues. ISACA Journal volume 6, 2001.

Marcella, A. 1998. Electronic Commerce – Part 1. [Online]. Available at Internet: http://www.itaudit.org/public_forum/f104ec.htm. Date visited: 27 October 1998.

Marks, N. 1998. Electronic Commerce - Part 2. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 25 April 2000.

Martin, D. 2000. Auditing Electronic Commerce Activities: Security Tools that should be in Place. [Online]. Available at Internet: http:www.itaudit.org. Date visited: 6 July 2001.

Martin1, D. 2000. Risk Management when Auditing E-commerce Activities. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

Masse, D.G. & Fernandes, A.D. 1997. Economic Modelling and Risk Management In Public Key Infrastructures. [Online]. Available at Internet: http://www.masse.org. Date visited: 7 June 2000.

Maung, P. 2001. Preparing for a Web Security Review. [Online]. Available at Internet: http://www/sans.org/infosecFAQ/audit/web_review.htm. Date visited 27 July 2001.

McDow, M. 2001. Secure Sockets Layer and Secure Electronic Transaction. [Online]. Available at Internet: http://gibson.nmhu.edu/~molly/papers/sslandset.htm. Date visited: 3 November 2001.

McGhie, L.L & Maier, P.Q. 1998. Security Management for the World Wide Web. Auerbach Publications 82-10-50 p1.

McNamee, D. 1995. The Role of the Internal Auditor and Performance Measurement. [Online]. Available at Internet: http://www.mc2consulting.com/perfmeas.htm. Date visited: 5 December 2001.

Mehta, R. 1999. Secure E-Business. *ISACA Journal volume I 2000* : 32 to 37.

Menkus, B. 1998. IS Auditing and EDPACS at 25 years. *EDPACS May 1998*. Auerbach Publications. 9-15.

Merriam-Webster. 1988. Webster's Ninth New Collegiate Dictionary. Merriam-Webster Inc, USA.

Messier, W.F. 2000. Auditing and Assurance Services – A systematic Approach. [Online]. Available at Internet: http://www.mhhe.com/business/accounting/messier/ppt/chpt01.ppt. Date visited: 14 April 2002.

Mika, S., Hochstetler, S., Tanner, H., Kulkarni, R. 2001. Extending Network Management Through Firewalls. [Online]. Available at Internet: http://www.ibm.com/redbooks. Date visited: 17 July 2001.

Miller, J. 2000. Information Systems Security: Lessons Learned. [Online]. Available at Internet: http://www.sana.org/infosecFAQ. Date visited: 27 July 2001.

Miller, L. N. 1999. Internal Audit's Critical Role – Part A. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

MilliCent. 2000. Why Millicent? [Online]. Available at Internet: http://www.millicent.digital.com/works/index.html. Date visited: 5 December 2001.

Moorestephens. 1997. Audit & Business Services. [Online]. Available at Internet: http://www.moorestephens.com/website/monaco.nsf/pages/mn-aud. Date visited: 8 February 2002.

Mossadams. 2002. Audit Services. [Online]. Available at Internet: http://www.mossadams.com/services/audit.htm. Date visited: 7 February 2002.

N

Neiger, D. 2000. How does E-commerce Work? [Online]. Available at Internet: http://www.neiger.com.au. Date visited: 23 January 2001.

Netscape. 1999. How SSL Works. [Online]. Available at Internet: http://developer.netscape.com/tech/security/basics/index.html. Date visited: 8 November 2001.

Netscape. 1999. Securing your site for E-Commerce. [Online]. Available at Internet: http://home.netscape.com/directorysc. Date visited: 7 December 1999.

Netscape. 2001. Encryption, and SSL. [Online]. Available at Internet: http://developer.netscape.com/docs/manuals/proxy/ProxyNT/security.htm. Date visited: 2 November 2001.

NHSD. 2002. Assurance Services. [Online]. Available at Internet: http://www.nshd.com/financial_reporting.htm. Date visited: 13 February 2002.

Nim. 1998. Maintain Physical Security. [Online]. Available at Internet: http://www.nim.com.au/security/se05001.htm. Date visited: 29 October 2001.

Norton, S. 2000. Circle of Security. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

O

OECD. 1998. The Economic and Social Impact of Electronic Commerce. [Online]. Available at Internet: http://www.oecd.org/subject/e-commerce. Date visited: 6 December 2000.

OECD. 1999. The OECD Principles of Corporate Governance. [Online]. Available at Internet: http://www.oecd.org/EN/home/0,,EN-home-28-nodirectorate-no-no--28,FF.html. Date visited: 7 January 2002.

Oliphant, A. 1998. An introduction to Computer Auditing. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 15 July 2000.

Oliphant, A. 1999. Managing Information Security. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 July 2001.

Oregon University. 2001. The Demand For Audit and Assurance Services; The CPA Profession. [Online]. Available at Internet: http://lcb1.uoregon.edu/alenikov/actg440/ch121.pdf. Date visited: 14 April 2002.

Oscar. 1999. E-Commerce Risks – Security and Business. [Online]. Available at Internet: http://oscar.cprost.sfu.ca/~isp253/992/netbucks/risks.htm. Date visited: 12 October 2001.

Overly, M.R. & Howell, C.T. 1998. Encryption: E-mail Security Over The Internet. [Online]. Available at Internet: http://www.foleylardner.com/LNU/ecomm.html. Date visited: 1 November 2001.

Owen, L. 1994. The Future of Information Systems Audit and Control. *IS Audit & Control Journal, Volume IV, 1994*. Information Systems Audit and Control Association.

Oxford Dictionary. 1984. The Pocket Oxford Dictionary. Seventh edition. Clarendon Press, Oxford.

P

Paliotta, A.R. 1995. Protecting the Electronic Environment in the 'New Technological World Order'. *ISACA Journal, Volume VI, 1995*: 6.

Paliotta, A.R. 1999. A personal view of a World Class IT Auditing Function. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

Paliotta, A.R. 2001. Cybersecurity and the Future of E-commerce. *IS Audit & Control Journal, Volume 2, 2001*. Information Systems Audit and Control Association.

ParkHill. 2002. Audit Approach and Quality. [Online]. Available at Internet: http://www.parkhill.org.uk/audit.html. Date visited: 5 February 2002.

Pathak, J. 2000. IT Audit Approach, Internal Controls, and Audit Decisions of an IT Auditor. [Online]. Available at Internet: http://www.theiia.org/itaudit/index.cfm. Date visited: 30 November 2001.

PCIS – Partnership for Critical Infrastructure Security. 2000. Consensus Roadmap for Defeating Distributed Denial of Service Atttacks. [Online]. Available at Internet: http://www.sans.org/ddos_roadmap.htm. Date visited: 18 November 2001.

Pei, G.S. 2001. E-Commerce Security: Cryptography with SET and SSL. [Online]. Available at Internet: http://www.cs.jcu.edu.au/~pei/cryptography.htm. Date visited: 5 November 2001.

Peixian, L. 2000. Popular Technologies & Open Issues in Securing Electronic Commerce. [Online]. Available at Internet: http://www.people.virginia.edu. Date visited: 9 October 2001.

Perry, W.E. 1983. Auditing Information Systems – A Step-by-Step Audit Approach. EDP Auditors Foundation – Audit Guide Series.

Perry, W.E. 1988. An Introduction to EDP Auditing. EDP Auditing Article number 72-01-01. Auerbach Publishers Inc.

Pethia, R., Crocker, S., Fraser, B. 1991. Guidelines for the Secure Operation of the Internet. [Online]. Available at Internet: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1281.html. Date visited: 30 October 2001.

Phifer, G., Smith, D., Meehan, P., Terhune, A. & Lombardo, D. 1998. Internet Strategies (INET) – Strategic Analysis Report. [CD-ROM], 26 October 1998. Abstract from: Gartner Group Abstracts Item: 007171233.

Pomeranz, F. 1992. The Successful Audit. Richard D Irwin, Inc, USA: 73.

Potter, C. 2001. Managing E-Business Risk – A UK Perspective [Online]. Available at Internet: http://www.ITAudit.org. Date visited: 10 January 2001.

PriceWaterhouseCoopers (PWC). 1998. Technology Forecast 1999. Published by PWC Technology Centre, California, USA, October 1998: 191 – 237.

PriceWaterhouseCoopers (PWCGlobal). 1999 Electronic Business Outlook. [Online]. Available at Internet: http://www.e-business.pwcglobal.com. Date visited: 20 August 2000.

PWC. 2000. Securing the Internet Economy. Infoworld: 3, 23, 26-30, 43-45.

PWC. 2001. Assurance and Business Advisory Services. [Online]. Available at Internet: http://www.pwcglobal.com/ie/eng/about/svcs/im/svcs/audit.html. Date visited: 26 February 2002.

PWC. 2001. Risk Management Forecast. PricewaterhouseCoopers LLP: 7.

Q

R

Rademacher, L. & Tunstall, B. 1998. Virtual Private Networks: Building Secure Data Tunnels Through The Internet. *EDPACS July 1998 Vol, XXVI, No. 1.* Auerbach Publications: 1-6

Ramos, D. 2001. The Auditor's Role in IT Governance. *Information Systems Audit and Control Journal Volume 5 2001.* Published by the Information Systems Audit and Control Association.

Rapp, G. 2001. How Safe Is My Money Online?. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

Restell, P. 2001. BS 7799 - Information Security Management. [Online]. Available at Internet: http://www.bsi-global.com. Date visited: 28 July 2001.

Robert Patrick. 2002. Your Internal Audit Department. [Online]. Available at Internet: http://www.myauditor.net.futuresite.register.com. Date visited: 25 February 2002.

Robertson Stephens & Co. 1997. Commerce by Numbers. [Online]. Available at Internet: http://www.computerworld.com/home/Emmerce.nsf/All/pop report (12/97). Date visited: 3 February 1999.

Roget. 1980. Roget's II The New Thesaurus. Houghton Mifflin Company, USA.

RSA. 2001. What are Certificate Revocation Lists (CRLs)?. [Online]. Available at Internet: http://www.encryption.com/rsalabs/faq/4-1-3-16.html. Date visited: 4 November 2001.

Rutgers. 1998.'Risks and Securities of On-line Information Flows. [Online]. Available at Internet: http://www.rutgers.edu/Accounting/raw/mikos. Date visited: 27 October 1998.

Rutgers. 2002. The Big Five. [Online]. Available at internet: http://accounting.rutgers.edu/raw/internet/big5.htm. Date visited: 6 June 2002.

S

SAICA. 1998. SAAS 401 - Auditing in a Computer Environment. The South African Institute of Chartered Accountants, Johannesburg.

Sayana, S.A. 2002. The IS Audit Process. *Information Systems Audit and Control Journal Volume 1 2002*. Published by the Information Systems Audit and Control Association.

Scacchi, W. The Emergence of Electronic Commerce on the Internet. 1995. [Online]. Available at Internet: http://www.usc.edu/dept/ATRIUM/Papers/EC_on_the_Inet.html. Date visited: 1 June 1999.

Scit. 1998. Security Issues Concerning the Information Age. [Online]. Available at Internet: http://www.scit.wlv.ac.uk/~c9576956/index.html. Date visited: 29 October 2001.

Siebel, T.M. & House, P. 1999. Cyber Rules - Strategies for Excelling at E-business. May 1999 – Currency and Doubleday, New York: 50-53.

Siegel, C.A. 1997. Managing Risk in Electronic Commerce. Auerbach 82-10-26: 1.

Singapore government. 1999. What is Electronic Commerce. [Online]. Available at Internet: http://www.ec.gov.sg. Date visited: 15 June 2001.

Sinnreich, A.; Sacharow, A; Salisbury, J.; Johnson, M. 1999. Creating New Business Models with Digital Rights Management. [Online]. Available at Internet: Http://www.strategis.ic.gc.ca. Date visited: 15 October 2001.

Soberman. 2002. Audit & Accounting / General Tax / Business Advisory. [Online]. Available at Internet: http://www.soberman.com/services/practice_audit.htm. Date visited: 12 February 2002.

Southcentre. 2000. E-commerce. [Online]. Available at Internet: http://www.southcentre.org/publications/ecommerce/ecommerce-04.htm. Date visited: 28 May 2001.

SSE. 2001. Certificate Revocation Lists. [Online]. Available at Internet: http://www.sse.ie/intro/crl.html. Date visited: 6 November 2001.

Stein, D.M., Arunachalam, V., Rittenberg, L.E. 2001. Electronic Commerce System Sophistication and the Audit Process. *IS Audit & Control Journal, Volume 1, 2001*. Information Systems Audit and Control Association.

Steinfeld, C. 2000. Electronic Commerce: An Introduction to the Special Issue. [Online]. Available at Internet: http://jcmc.huji.ac.il. Date visited: 5 June 2001.

Stewart, T.R. 1998. Selected E-business Issues. [Online]. Available at Internet: http://www.dttus.com. Date visited: 20 September 2001.

Strategis. 2001. Introduction to E-commerce. [Online]. Available at Internet: http://www.strategis.ic.gc.ca. Date visited: 5 June 2001.

Suffolkacct. 2002. The Risk Based Audit Approach. [Online]. Available at Internet: http://www.suffolkacct.org/lshaw/acct332/Chapter11/sld019.htm. Date visited: 5 February 2002.

Sun. 1998. X.509 Certificates and Certificate Revocation Lists (CRLs). [Online]. Available at Internet: http://java.sun.com/products/1.2/docs/guide/security/cert3.html. Date visited: 7 November 2001.

Symantec. 2000. Internet Security for the Web. [Online]. Available at Internet: http:www.symantec.com. Date visited: 15 May 2001.

T

TEA Division of School Audits. 2002. Who Can Perform an Audit? [Online]. Available at Internet: http://www.tea.state.tx.us/school.finance/audit/resguide7/audit/audit-02.htm. Date visited: 4 June 2002.

Techguide. 2000. Technology Guide - Internet Security Primer. [Online]. Available at Internet: http://www.techguide.com. Date visited: 17 May 2001.

Terena. 2001. Security and Encryption. [Online]. Available at Internet: http://www.terena.nl/libr/gnrt/security/s1.html. Date visited: 1 November 2001.

Tibaldeo, G. & Buben, D. 1996. Cashing in on Technology: A Primer on Electronic Payment Systems. *IS Audit & Control Journal,* Volume VI, 1996: 14–18.

Todd, B. 2000. Distributed Denial Of Service Attacks. [Online]. Available at Internet: http://www.opensourcefirewall.com/ddos_whitepaper_copy.html. Date visited: 5 November 2001.

Tremblay, R. 2000. Host Security Considerations. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 9 October 2001.

Tufts. 2002. Audit Management Advisory Services. [Online]. Available at Internet: http://www.tufts.edu/central/internalaudit/audit/process.htm. Date visited: 25 February 2002.

Tyson, J. 2001. How Firewalls Work. [Online]. Available at Internet: http://www.howstuffworks.com. Date visited: 21 October 2001.

Tyson2, J. 2001. How Virtual Private Networks Work. [Online]. Available at Internet: http://www.howstuffworks.com. Date visited: 22 October 2001.

U

UDEL. 2002. Auditing Notes – Chapter One. [Online]. Available at Internet: http://udel.edu/~firehead/acct417/Act-Notes/Act-01.pdf. Date visited: 4 June 2002.

UIS. 2001. The Role of the Public Accountant in the American Economy. [Online]. Available at Internet: http://people.uis.edu/jnosa1/chp01.ppt. Date visited: 14 April 2002.

Unixtools. 2001. Unix Computer Security. [Online]. Available at Internet: http://www.unixtools.com/security.html. Date visited: 6 November 2001.

USD (University of San Diego). 2002. 'Big Five' CPA Firms. [Online]. Available at Internet: http://www.sandiego.edu~dvasquez/big5.html. Date visited: 11 June 2002.

US Department of Commerce. 1998. The Emerging Digital Economy – Chapter 1 [Online]. Available at Internet: Http://www.ecommerce.gov/viewhtml.htm. Date visited: 2 June 1999.

V

VAG – Victorian Auditor General Office. 2001. Victorian Auditor General Website. [Online]. Available at Internet: http://www.audit.vic.gov.au/agmrole.htm. Date visited: 30 November 2001.

Vallabhaneni, R.S. 1991. CISA Exam Preparation Manual. Published by the *Information Systems Audit and Control Association:* Chicago: 6 – 11.

Vandenoever, C. 1995. Information Protection, your Business and the Internet. Deloitte &Touche LLP.

Van der Walt, A. Strydom, J.W. Cant, M.C. Jooste, C.J. 1997. Marketing Management, 4th Edition, Juta &Co.

Verisign. 1999. Securing Your Web Site For Business. [Online]. Available at Internet: http://www.verisign.com/rsc/gd/srv. Date visited: 8 October 1999.

Vining. P. 2001. Audit Department. [Online]. Available at Internet: http://fac.mgmt.virginia.edu/minutes/EmpCouncil\EC042001.htm. Date visited: 4 June 2002.

VISA. 1997. Book 1: Business Description SET Secure Electronic Transaction Specification. [Online]. Available at Internet http://www.visa.com. Date visited: 26 June 1998.

VISA. 1998. SET – The Key to Safe Shopping. [Online]. Available at Internet: http://www.visa.com. Date visited: 29 June 1998.

W

Walden, I. & Braganza, A. 1993. EDI Audit and Control. NCC Blackwell Ltd, Oxford, England: 19 – 30.

Walder, B. 1999. Internet Security. [Online]. Available at Internet: http://www.nss.co.uk. Date visited: 23 July 2001.

Warigan, S. 1999. Commercial, Privacy Protection, Regulatory, and Security Implications of Electronic Cash. Auerbach Publications – CRC Press LLC: 16 to 19.

Westwood. 1997. What is the Role of Internal Auditors? [Online]. Available at Internet: http://plaza27.mbn.or.jp/~westwood/9708diry.htm. Date visited: 7 January 2002.

Whatis. 2000. IT-Specific Encyclopedia. [Online]. Available at Internet: http://whatis.com. Date visited: 19 October 2000.

Widman, L.E. 1999. Privacy and Security on the Internet. [Online]. Available at Internet: http://www.med.edu-com/internet-security.html. Date visited: 5 November 2001.

Wilkinson, Cerullo, Raval, Wong-On-Wing. 2001. Accounting Information Systems: Essential Concepts and Applications. [Online]. Available at Internet: http://www.utm.edu/~ejoyner/classes/acct1461/a1461-10.ppt. Date visited: 14 April 2002.

Wilson, J.D. & Root, S.J. 1983. Internal Auditing Manual. Warren Gorham & Lamont: 1-1 to 1-23.

Wilson, S. 1999. Current issues in the rollout of a National Authentication Framework. [Online]. Available at Internet: http://www.acs.org.au/president/1998/past/io98/rllot.htm. Date visited: 17 October 2001.

Wladawsky-Berger, I. 1997. Keynote Speech at Summer Internet World 97. [Online]. Available at Internet:http://www.ibm.com/news/archive/stories/1997/iw5.html. Date visited: 7 November 1999.

World Book Encyclopedia. 2001. Audit. World Book Inc, Chicago: 884.

WUStL (Washington University of St Louis). 2000. Types of Audits. [Online]. Available at Internet: http://internalaudit.wustl.edu/audittypes.html. Date visited: 2 December 2001.

X

Y

Yaacov, N. 1997. Certificate Revocation and Certificate Update. [Online]. Available at Internet: http://www.usenix.org/publications/library/proceedings/sec98/full_papers/nissim/nissim.html. Date visited: 27 October 2001.

Yasuda, M. 1997. Certification Authority Guidelines in Japan. [Online]. Available at Internet: http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/92. Date visited: 27 October 2001.

Z

Zdnet. 1997. Disarming the Net - How Encryption Works. [Online]. Available at Internet: http://www.zdnet.com/pcmag/features/inetsecurity/howencrypt.htm. Date visited: 6 November 2001.

Zdnet2. 1997. Disarming the Net - Authentication. [Online]. Available at Internet: http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm. Date visited: 6 November 2001.

Zeus. 2001. Increasing Security, Reducing Workload. [Online]. Available at Internet: http://www.zeus.co.uk/library/articles/security.html. Date visited: 12 October 2001.

Zimits, E.C. & Montano, C. 1998. Public Key Infrastructure: Unlocking the Internet's Economic Potential. [Online]. Available at Internet: http://www.iword.com/iword32/istory32.html. Date visited: 14 August 1999.

Zwicky, E.D., Cooper, S., & Chapman, D.B. 2000. Building Internet Firewalls. O Reilly & Associates Inc. 2nd Edition. USA.

Summary

Candidate: Pieter Stefan Bezuidenhout
Study Leader: Prof. Dr. J.D. Gloeck
Department: Department of Auditing
Degree: Magister Commercii
Title: An audit approach of the information systems auditor in an electronic commerce environment with emphasis on internet payment security

Electronic Commerce (EC) is a growing business option and due to the "openness" of the underlying technologies used for EC, introduces new risks and new technologies that require sophisticated and sometimes very technical controls to be implemented. The role of the IS auditors is to ensure that they are technically competent to understand the impact of new technologies on the control environment and at the same time IS auditors need to be able to communicate the audit results to non-technical management.

In this study the following framework, supported by detailed information and procedures for each step, is provided to assist the IS auditor to formulate an appropriate audit approach for an EC payment security audit:

- Gathering of background information related to EC payment security.
- Highlighting the risks in this environment.
- Identifying possible controls that will minimise the risks.
- Attending to various audit considerations that should be addressed by the IS auditor (these considerations are based on the underlying technologies, general controls, and EC-specific issues e.g., PKI, digital certificates, etc.).

The study highlighted the fact that the IS auditors should understand that they can not be experts in all the different technologies related to EC payment security. They should, however, equip themselves with the knowledge to understand the risks involved with new technologies and they should have a sufficiently in depth background exposure to technology to understand the controls required to address the risks. Results of previous audit procedures also play a significant role in shaping the IS auditor's approach when auditing in an EC payment security environment.

This thesis provides the IS auditor with a holistic approach to an EC payment security audit. After considering and implementing the elements of the framework developed in this study in an EC payment security audit, the IS auditor has to perform the actual audit tests, evaluate the results, and report the findings. Detailed audit considerations have also been provided to assist the IS auditor in collecting information and in developing an audit program.

Opsomming

Kandidaat: Pieter Stefan Bezuidenhout
Studieleier: Prof. Dr. J.D. Gloeck
Departement: Ouditkunde
Graad: Magister Commercii (Rekenaarouditering)
Titel: 'n Ouditbenadering van die inligtingstelselouditeur in 'n elektroniese handel omgewing met klem op internetbetalingsekuriteit

Elektroniese handel (EH) is 'n groeiende besigheidsopsie en as gevolg van die "oop" struktuur van die onderliggende tegnologieë wat gebruik word in EH, word nuwe risiko's en nuwe tegnologieë bekendgestel wat die implementering van gesofistikeerde en telkens baie tegniese kontroles vereis. Die rol van die inligtingstelsel (IS) ouditeure is om te verseker dat hulle tegnies bekwaam is om die impak van die nuwe tegnologieë op die kontrole omgewing te verstaan, en terselfdertyd moet IS ouditeure in staat wees om die resultate van die oudit aan nie-tegniese bestuur te kommunikeer.

In hierdie studie word die volgende raamwerk, wat ondersteun word deur gedetailleerde inligting en prosedures vir elke stap, verskaf om die ouditeur by te staan met die formulering van 'n toepaslike ouditbenadering vir 'n oudit van EH-betalingsekuriteit:

- Versameling van agtergrondinligting in verband met EH-betalingsekuriteit.
- Identifisering van die risiko's in die omgewing.
- Identifisering van moontlike kontroles wat die risiko's sal minimaliseer.
- Gee aandag aan die verskeie ouditaspekte wat deur die IS ouditeur oorweeg behoort te word (hierdie oorwegings is gebaseer op die onderliggende tegnologieë, algemene kontroles en spesifieke EH-kwessies byvoorbeeld, openbare sleutel infrastruktuur (PKI), digitale sertifikate, ens.).

Hierdie studie beklemtoon die feit dat IS ouditeure moet verstaan dat hulle nie deskundiges kan wees in al die verskillende tegnologieë wat met EH-betalingsekuriteit verband hou nie. IS ouditeure behoort egter hulleself toe te rus met die kennis om die risiko's wat by die nuwe tegnologieë betrokke is, te verstaan en

hulle behoort voldoende diepte agtergrondblootstelling aan die tegnologieë te hê om die vereiste kontroles wat die risiko's sal beperk, te verstaan. Die resultate van vorige ouditprosedures speel ook 'n belangrike rol in die formulering van die ouditeur se benadering wanneer 'n oudit uitgevoer word in 'n EH-betalingsekuriteitomgewing.

Hierdie studie verskaf 'n holistiese benadering aan die IS ouditeur vir 'n EH-betalingsekuriteitoudit. Nadat die elemente van die raamwerk wat in hierdie studie van 'n EH-betalingsekuriteitomgewing ontwikkel is, oorweeg en geïmplementeer is, moet die IS ouditeur die werklike ouditttoetse uitvoer, die resultate evalueer en bevindinge rapporteer. Detail oorwegings is ook verskaf om die IS ouditeur te help tydens die proses van inligtingsversameling en die ontwikkeling van die ouditprogram.