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.