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.