An audit approach to e-commerce payment security

PS Bezuidenhout
Department of Auditing
University of Pretoria

JD Gloeck
Department of Auditing
University of Pretoria

ABSTRACT

This is the second of two articles that address the audit approach to EC payment security. The previous article (Bezuidenhout & Gloeck, 2003) dealt with the following:

- The EC payment security environment, and
- The risks prevalent in this environment.

This paper capitalises on the first article and uses the identified risk model to develop an audit approach for the IS auditor that can be used when he/she is engaged in the audit of an e-commerce (EC) payment security environment. As part of the research various audit approaches followed by selected audit firms, are presented and the commonalities of these approaches are translated into steps that the IS auditor should follow as part of his/her audit approach to EC payment security.

Key words

Audit of… information systems, internet security, internet payment; e-commerce; information systems auditor/audit; internet payment security; internet payment methods; internet risk management; internet security risks; IS auditor approach.

1 BACKGROUND INFORMATION

1.1 Reference to previous research

Electronic commerce is a relatively new, technology-based business phenomenon, which will be important to future business and therefore to the Information Systems (IS) auditor. There are many aspects to 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. EC payment environment risks stem from the fact that the Internet has been designed to be "open", which increases the likelihood of manipulation (For a full discussion on these aspects refer Bezuidenhout & Gloeck (2003)). Security and control in this environment is critical. The IS auditor needs to approach an audit of EC payments in a structured way to ensure that all the vulnerabilities have been addressed.

Bezuidenhout & Gloeck (2003) highlighted the fact that the IS auditor needs to be aware of the inherent risks in an EC payment security environment to enable him/her to evaluate/review such risks. The authors also showed that the IS auditor plays an important role in the risk management process through the risk identification process and associated identification and evaluation of the controls required to minimize or manage such risk.

1.2 Objective of this research

The objective of this research is to develop and define an audit approach for the IS auditor that can be used when he/she is engaged in the audit of an e-commerce (EC) payment security environment. The research also highlights the risk identification process as an integral part of the audit approach.

Another objective of this research is to present the various audit approaches followed by selectedaudit firms, and to translate the commonalities of these approaches into steps that the IS auditor should follow as part of his/her audit approach to EC payment security.

1.3 Overview

This article is structured as follows:

1. Firstly, an acceptable audit approach is defined by highlighting the approaches of the major firms performing external, public audit and accounting

services, as well as selected internal audit departmental approaches;
2. Secondly, the audit steps to be followed are identified as part of the audit approach; and
3. Thirdly, an overview is provided describing 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 outside the scope of this article, mainly due to the high number of audit areas involved, as well as the complexity of the areas. As part of a comprehensive Masters dissertation, Bezuidenhout (2002) defined detailed procedures specifically relating to EC payment security.

2 AUDIT APPROACH

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 referred to later, the above 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).

2.2 The elements of the audit approach

2.2.1 Audit approaches by major accounting firms

The audit approaches of the major audit and accounting firms were chosen for further analysis because they 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 (listed alphabetically):

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

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

The Arthur Andersen approach:

"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).

The Deloitte & Touche approach states (Deloitte, 2001):

"…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).

2.2.1.1 Summary of the audit approaches of the major accounting firms

From the audit approaches of the "Big 5" accounting firms summarised above, 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;
- 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 have been identified, including the nature and extent of audit procedures, what remains is performing the audit tests, evaluating and reporting on the findings. The process is iterative as well: where testing reveals other risks that need to be addressed, the new risks then need to be included in the full audit approach cycle.

2.2.2 Audit approach as prescribed by professional associations

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.
- Conclude the audit.

The IS auditor's approach to an audit, including an audit of EC payments security, is also defined by professional associations 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 to be inter-dependent. The output of each step serves as the input for the following step. For example, the controls identification process cannot take place effectively without the risks being identified.

It is clear from the audit approaches followed by the professional organisations as highlighted above, that they correspond to the approaches followed by the major accounting firms identified in 2.2.1 above.

2.2.3 Audit approaches followed by other organisations

The following are examples of a selection of internal audit departments' audit approaches:

- A risk based audit approach is used by Suffolk (Suffolkacct, 2002). It involves the following four steps:
  - o determine the threats;
  - o identify the control procedures that should be in place to minimise each threat;
  - o evaluate the control procedures;
  - o 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) as involving 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 consisting of the following steps:
  - 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."

The above statements clearly show that there are commonalities in the approaches used by the major external audit and public accounting firms and in individual companies' internal audit departments. These common steps are used in this article to develop and define a generic audit approach that can be followed when auditing EC payment security, and are identified in Section 3 below.

3 COMMON STEPS IN THE EC PAYMENT SECURITY AUDIT APPROACH

The audit approaches followed by the major accounting firms, professional associations, 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 article 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;
- 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 the first article (Bezuidenhout & Gloeck, 2003), the Internet is considered to be an inherently high risk area. The timing of the audit procedures for EC payment security is therefore of such a crucial 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, and 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;
- The nature of risks in the environment.

An audit approach is further influenced by 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 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 be of greater reliability than others (Abrema, 2002). This article is ostensibly about the formulation of the audit approach. It therefore necessarily excludes any discussion of the detail the audit considerations Detailed audit considerations 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 addressed. For the practical reason of space, these details are not listed here.

4 CONSIDERATIONS ON AUDIT PROCEDURES FOR AN EC PAYMENT SECURITY AUDIT

4.1 Step 1 - scope and understand the environment - background information gathering

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 scanners to determine vulnerabilities not detectable in any other way;
- The results of previous audit procedures – this will be addressed below.

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 and a starting point to the audit. Other factors that need to be determined include identifying 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 which include interviews with the auditee, together with reviews of published material and material available from the auditee or his vendors. 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 vendors' product manuals provided with their hardware or software, and published books.

4.1.1.1 General IT environment information gathering

There are many information-gathering guidelines available related to the general IT environment, that can be used to obtain a general understanding of the IT environment. The IS auditor also needs to gather information on specific aspects such as hardware platforms, external links, operating systems used, outsourced functions, tools used (e.g., network scanning and intrusion detection), etc. However, the auditor will need EC-specific information to understand how EC-related technology fits into the overall environment.

4.1.1.2 EC specific information gathering considerations

EC specific information gathering considerations include information on the control environment, business practice disclosures, transaction integrity controls, information protection controls, legal considerations and specific rules. The last two items are detailed below:

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 (ICAS, 1998):

- 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 numerous other major issues that need to be addressed. As indicated in his dissertation (Bezuidenhout, 2002), 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 protection 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 so linked have to agree? Do links constitute a breach of copyright? In principle, viewing a site involves copying its content to a cache on the viewer's computer/server. Is there an implied license to view by web site owners? Does this extend to downloading and printing?
- **Security**: how far do professional service suppliers, for example accountants or lawyers, have to go to ensure a web site is secure, hacker-free and virus-free etc? If this is not achieved, is this a breach of clients' rights to confidentiality?
- Are there any issues around **data protection**? Any business storing personal data (including emails) may need to guard against cross border data flows to non-data-protection regimes (companies as well as countries), as, for example, is happening in 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.

4.1.1.4 Special rules

New ways to conduct electronic business often mean 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 further, prevents service providers from alerting them to such occurrences.

The IS auditor should therefore understand the client's business philosophy, strategy and processes. Central to this is a detailed understanding of the impact of technology on 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, if the server and the fulfilment facilities are physically in different countries and under different legal systems?

At the end of this phase the IS auditor should have sufficient information and understanding to continue to the next step of developing 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.

4.2 Step 2 - risk analysis considerations

The risk analysis considerations in an EC environment have been identified and described in detail in the first article in this two-part series (Bezuidenhout & Gloeck, 2003). The risks present in the EC payment security environment may be identified by using the information gathered in the background information gathering phase of the audit, by brainstorming, by drawing on past experience, and by referring to 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 4.2.1 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 all high risk areas are addressed. If audit time allows, medium and low risk areas should also then be considered.

4.2.1 Results of previous audit procedures

As already indicated, 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 or z/OS, 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 have been 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 should also assess management actions taken since the last audit/ review.

4.2.2 Risk considerations for EC payment security

As shown in the first article (Bezuidenhout & Gloeck, 2003), 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 4.3 below) will identify controls to mitigate these risks.

4.3 Step 3 - control considerations

As stated in the risk section (4.2.1) 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 4.2.1 above, will determine if any additional focus is required in those areas when conducting an EC payment security audit.

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 1.1 below represents a summary of important conclusions regarding the audit approach. 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 the previous article (and mentioned in 4.2.2 above) and have been included below the table for ease of reference. The reference column refers to the control procedures section that follows the table. 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 1.1 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	4.3.2.1
Physical and environmental security	X	X	X	X	X	X	4.3.2.2
Operating system and web server vulnerabilities/controls	X	X	X	X	X	X	4.3.2.3
Change management	X	X	X	X	X	X	4.3.2.4
Business continuity planning	X	X	X	X	X	X	4.3.2.5
Organisational structure	X	X	X	X	X	X	4.3.2.6
Computer operations and backup	X	X	X	X	X	X	4.3.2.7
Legal compliance	X	X	X	X	X	X	4.3.2.8
Event Journalling	X	X	X	X	X	X	4.3.2.9
Controls\Risks	**1**	**2**	**3**	**4**	**5**	**6**	**Reference**
Technical EC controls							
Encryption, privacy, and secure protocols[*1]		X	X		X	X	4.3.3.2
Digital certificates/signatures[*1]	X	X			X	X	4.3.3.3
Firewall and router considerations	X			X			4.3.3.1
Public Key Infrastructure (PKI)		X	X	X	X	X	4.3.3.3
Intrusion Detection Systems	X			X			4.3.3.4
Virtual Private Networks (VPN)[*2]	X		X	X			4.3.3.5

*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.

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.

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 perceived or actual risks encountered. Due to the complexity of the technology in the EC payment security environment, and the vast number of details required to provide accurate considerations, these have not been included in this article. Bezuidenhout (2002) defined the detailed procedures specifically related to EC payment security.

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 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 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 are mentioned in the PKI section (4.3.3.3) below.

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 have been included in such a previous audit, including aspects mentioned in this section. Where weaknesses are 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 outline 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. Such assessments should provide for effective augmentation of existing security programs, and the implementation of new security measures and countermeasures. Security administration also includes monitoring activities related to intrusion detection, and this is covered under Section 4.3.3.4 below.

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 and would include items such as environmental controls (e.g., air conditioning), asset control, and physical access.

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. Where weaknesses are 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.

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 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 such as file and directory access control, patch management, network services, logical security, logging, backup, installation procedures, etc. have been included in previous audit procedures. Where weaknesses have been 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.

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 their attempts to secure their software and/or hardware, or write in their policies, they have no control over the end user's computer. That computer could store all the digital certificates, most of the consumers' personal information, and quite often, usernames and passwords. People often 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 includes physical security, access controls and policies as mentioned in Sections 4.3.2.1 and 4.3.2.2 above.

4.3.2.4 Change management

A change management review would normally be performed as a separate audit. 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. Where weaknesses are 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 change management review would include aspects such as approval, segregation of duties, etc.

4.3.2.5 Business continuity planning (BCP)
Audit considerations

A BCP review would normally be performed as a separate audit and would include aspects such as contingency planning, testing, emergency procedures, etc. especially related to EC payment-specific issues. 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 key considerations that need to be taken into account by the IS auditor. Where weaknesses are 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 policies and procedures should be in place to ensure the continuity of service to customers in the event the CA terminates.

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 complied with.

The audit procedures related to intrusion detection (i.e., the monitoring responsibility of staff) is covered in more detail in Section 4.3.3.4 below.

4.3.2.7 Computer operations and backup
Audit considerations

A computer operations and backup review would normally be performed as a separate audit and would include aspects such as documented procedures, segregation of duties, capacity planning, data backup, operator logging and monitoring, etc. 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 highlight key (critical) issues that need to be taken into account by the IS auditor. Where weaknesses are 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.

4.3.2.8 Legal compliance
Audit considerations

As stated in Section 4.1.1.3 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 process have been included in such a review. Apart from the procedures in the relevant section mentioned above, the auditor should also 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.

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 complied with:

Review event journal and assessment reports and ensure the following are specified:

- 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 archiving of the event journal;
- Archiving 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.

4.3.3 EC specific technical security control considerations

4.3.3.1 Firewall and router considerations

A router and/or firewall audit would normally be performed as a separate audit and would include aspects such as configuration, administration, and monitoring procedures, change management, recoverability, etc. The purpose of addressing this area in an EC payment security audit is not to evaluate all the aspects used for control purposes, but rather to consider aspects that need to be taken into account by the IS auditor. Where weaknesses have been identified in a previous review, 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.

4.3.3.2 Encryption, privacy, and secure protocols

Encryption is regarded as a very important control for EC payment security. 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. Also included in an audit are aspects such as protection of information during transmission.

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

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 below 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. 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 (e.g. SAS 70 reports)) related to the CA 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:

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 Re-key
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Revocation List (CRL) Processing

4.3.3.4 Intrusion detection
Audit considerations

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. Some of the considerations would be covered in an operating system/server vulnerability review or a firewall review. The IS auditor needs to ensure that intrusion detection aspects were covered by the appropriate reviews. This is normally done by evaluating the results of such reviews and evaluating the impact of negative findings on the risks in the intrusion detection area.

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 the connections 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 4.3.3.1 above.
- **Encryption** – encryption was discussed in detail in Section 4.3.3.2 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 Section 4.3.3.2 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.

5 CONCLUSION

EC is a growing business option and due to the “openness” of the underlying technologies used for EC, it introduces new risks and new technologies that require sophisticated and sometimes very technical controls to be implemented. Electronic commerce is a broad and varied field prone to technical complexity.

In order to understand and assess controls in this environment IS auditors are forced to continuously update their skills and to provide management of an organisation with assurance on the control environment for this new technology. 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. Consequently, there have been numerous developments in the audit area that provide guidance to the IS auditor operating in an EC environment.

The audit approach directs the IS auditor to follow certain steps when performing an audit. This article showed how such an audit approach for the IS auditor, auditing EC payment security, is developed. As indicated in this article, the audit approaches followed by the major public accounting firms, as well as numerous other audit organisations and departments, are risk-based and involve the following steps:

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

The remaining steps and procedures required by an IS auditor are:

- To perform audit tests;
- Evaluate the results of the tests;
- Report on any findings.

This article 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 article, the audit of EC payment security involves a very wide spectrum of technologies and includes many audit areas. Many of the technologies, if correctly used, will aid in securing EC payments. The responsibility 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, and to base his/her work thereon.

Once the IS auditor understands the available technologies and the controls they provide, this enables him/her to develop an appropriate audit approach. The results of previous audit procedures play an important role in reducing the number of areas to audit and amount of work required to be done, enabling the IS auditor to focus the audit efforts for greater efficiency and effectiveness.

This article provides an easy-to-use table (in Section 3.3) in which risks and controls are linked. This table may also serve as a guide to the IS auditor to identify the major areas of an audit in the EC payment security environment. This article shows the complexity of interconnected business processes and the audit requirements of each as it enters the EC arena. 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 reliance may be placed on previous audit procedures.

6 THE ROLE OF THE AUDITOR IN EC PAYMENT SECURITY REVIEWS – FINAL THOUGHTS

The IS auditor has an ongoing responsibility to ensure that he/she keeps up to date with changes in technologies, especially changes related to EC and, in this specific case, EC payment security.

This is due to the fact that EC is constantly redefining current business processes, and technologies are changing exponentially. The IS auditors should continually assess his/her own procedures used to update him/herself regarding developments in EC and related technologies. As part of this process the IS auditor needs to identify processes to evaluate his/her own skills against the changing requirements brought about by developments in EC, and to supplement shortcomings with training (internal, external, or self-training).

Given the pace of change in the EC environment, allowing technological developments to get ahead of the IS auditor renders his/her service irrelevant. The key characteristic of an IS auditor is the ability to be at the forefront of technological developments as applicable to the EC environment. The IS auditor is then able to play a proactive role in assessing risks and controls, and advising management accordingly. The IS auditor's skills need to be more refined and more innovative than in a paper-based environment because EC technologies take the IS auditor into areas that have not been assessed before and where limited information is available.

By following the audit approach described in this article, the IS auditor is able to speed up the audit process and is better prepared to develop an audit program especially in areas where no precedent yet exists.

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. However, 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 assess the risks in the environment to an acceptable level of certainty. The IS auditor should therefore also be aware of new technologies that may be used to assist in the performance of the audit tests.

The IS auditor should understand that he/she cannot be an expert in all the different technologies related to EC payment security, nor remain an expert in any one technology unless there is constant, diligent research and training. The IS auditor should therefore arm him/herself with sufficient knowledge to understand the risks involved with new technologies and he/she should have a sufficiently in-depth theoretical background and exposure to technology to understand the controls required to address the risks. At the same time the IS auditor needs to be able to communicate the audit results to non-technical management.

Above all, the development and implementation of the correct audit approach in the EC environment is seen as the most crucial step in delivering efficient, effective and economical audits.

REFERENCES

AARF (Australian Accounting Research Foundation). 2000. *AGS 1056 – "Electronic Commerce: Audit Risk Assessments and Control Considerations*. *Australian Accounting Research Foundation (AARF)*: Melbourne: 6-8.

Abrema. 2002. Glossary of Auditing Terms. [Online]. Available at Internet: http://www.abrema.net/abrema/audit_approach_g.html. Date visited: 5 February 2002.

Accountants World. 2002. 'Big 5 Firms (5)'. [Online]. Available at http://www.accountantsworld.com/miscresources.asp?linktype=special&cat=Big+5+firms Date visited: 11 June 2002.

Andersen. 2002. 'Audit and Assurance Services'. [Online]. Available at Internet: http://www.andersen.com/website.nsf/content/EuropeIrelandIndustry9!OpenDocument. Date visited: 8 February 2002.

Bezuidenhout, P.S. & Gloeck, J.D. 2003. *Identifying risks in e-commerce payment security for use by the IS auditor. The Southern African Journal of Accountability and Auditing Research*. Volume 4: 2003: 21-36.

Bezuidenhout, P.S. 2002. *An Audit Approach Of The Information Systems Auditor In An Electronic Commerce Environment With Emphasis On Internet Payment Security*. Unpublished Masters dissertation. University of Pretoria.

Business Majors. 2002. Major Accounting Firms. Available at Internet: http://businessmajors.about.com/cs/accountingfirms. Date visited: 11 June 2002.

CPGCA. 2001. Auditing. [Online]. Available at Internet: http://www.cpgca.co.za/auditing.htm. Date visited: 7 February 2002.

CSU (Colorado State University). 2002. Colorado State University Libraries Business Details. [Online]. Available at http://patriot.library.colostate.edu/research/business/resourceDetail.php?resourceID=19. Date visited: 11June 2002.

Deloitte. 2001. Our Audit Approach and Technology. [Online]. Available at Internet: http://www.deloitte.com.ky/assuranceapproach.htm. Date visited: 5 February 2002.

Emich (Eastern Michigan University). 2002. 'Worldwide Fee Income of the Big Five'. [Online]. Available at http://www.emich.edu/public/accounting/big5.htm. Date visited: 11June 2002.

EIU. 2002. Big 5 CPA Firms. [Online]. Available at http://www.eiu.edu/~ldudley/big5.htm. Date visited: 11 June 2002.

EY. 2002. 'Focused Approach'. [Online]. Available at Internet: http://www.ey.com/GLOBAL/gcr.ncf/Isle_of_Man/Audit_&_Assurance_Approach. Date visited: 5 February 2002.

IAPC (International Auditing Practices Committee). 2001. *Electronic Commerce Using the Internet or Other Public Network*'. IAPC.

iBig5. 2002. 'The Global Website for Alumni of the Big 5 Accounting Firms. [Online]. Available at http://www.ibig5.com/structure.cfm. Date visited: 11 June 2002.

ICAS - The Institute of Chartered Accountants in Scotland. [Online]. 'Discussion paper on Electronic Commerce'. Available at Internet: http://www.icas.org.uk/members/servicesfrom. Date visited: 14/7/1999.

Internalaudit. 2001. 'Our Typical Work Plan Approach'. [Online]. Available at Internet: http://www.internalaudit.co.uk/work.html. Date visited: 12 February 2002.

ISACA. 2001. *2001 CISA Review Technical Information Manual*. Information Systems Audit and Control Association: 20, 25, 30.

KPMG. 2000. 'Our Audit Approach'. [Online]. Available at Internet: http://www.kpmg.ie/audit/approach.htm. Date visited: 5 February 2002.

KPMG. 2002. 'Assisting Internal Audit'. [Online]. Available at Internet: http://ourworld.compuserve.com/homepages/BIverson/irm-ia.htm. Date visited: 15 February 2002.

Merriam-Webster. 1988. *Webster's Ninth New Collegiate Dictionary*. Merriam-Webster Inc, USA.

Moorestephens. 1997. 'Audit & Business Services'. Available at Internet: http://www.moorestephens.com/website/monaco.nsf/pages/mn-aud. Date visited: 8 February 2002.

Mossadams. 2002. 'Audit Services'. Available at Internet: http://www.mossadams.com/services/audit.htm. Date visited: 7 February 2002.

NHSD. 2002. 'Assurance services'. [Online]. Available at Internet: http://www.nshd.com/financial_reporting.htm. Date visited: 13 February 2002.

ParkHill. 2002. 'Audit Approach and Quality'. [Online]. Available at Internet: http://www.parkhill.org.uk/audit.html. Date visited: 5 February 2002.

PwC. 2001. Assurance and Business Advisory Services'. [Online]. Available at Internet: http://www.pwcglobal.com/ie/eng/about/svcs/im/svcs/audit.html. Date visited: 26 February 2002.

Robert Patrick. 2002. 'Your Internal Audit Department'. [Online]. Available at http://www.myauditor.net.futuresite.register.com. Date visited 25 February 2002.

Roget. 1980. *Roget's II The New Thesaurus*. Houghton Mifflin Company, USA.

Rutgers. 2002. 'The Big Five'. [Online]. Available at http://accounting.rutgers.edu/raw/internet/big5.htm. Date visited 6 June 2002.

SAICA. 1998. *SAAS 401 - Auditing in a Computer Environment*. The South African Institute of Chartered Accountants, Johannesburg.

Soberman. 2002. ‘Audit & Accounting / General Tax / Business Advisory’. [Online]. Available at Internet: http://www.soberman.com/services/practice_audit.htm. Date visited: 12 February 2002.

Suffolk. 2002. ‘The Risk Based Audit Approach’. [Online]. Available at Internet: http://www.suffolkacct.org/ Ishaw/acct332/Chapter11/sld019.htm. Date visited: 5 February 2002.

Tufts. 2002. ‘Audit Management Advisory Services’. [Online]. Available at Internet: http://www.tufts.edu/ central/internalaudit/audit/process.htm. Date visited: 25 February 2002.

USD (University of San Diego). 2002. ‘”BigFive” CPA Firms’. [Online]. Available at http://www.sandiego.edu~ dvasquez/big5.html. Date visited: 11 June 2002.