

University of Pretoria etd – Bezuidenhout, P S (2006)

Foreword

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

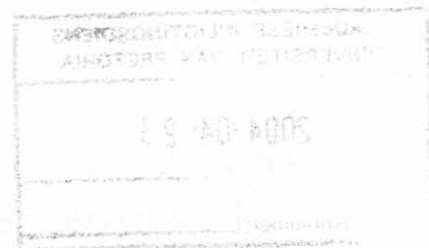
**BY**

**PIETER STEFAN BEZUIDENHOUT**

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

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

**OCTOBER 2002**



## Foreword

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

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

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

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

NEW YORK

14 October 2002.

## Contents

<b>CHAPTER 1 .....</b>	<b>1</b>
1.1 INTRODUCTION.....	2
1.2 BACKGROUND TO THE STUDY.....	3
1.2.1 FUNCTIONS OF THE DIFFERENT AUDITORS.....	3
1.2.1.1 The External auditor.....	3
1.2.1.2 The Internal Auditor.....	4
1.2.1.3 The Information Systems (IS) Auditor.....	4
1.2.2 BACKGROUND.....	5
1.2.2.1 A New-World Economy.....	5
1.2.2.2 Conclusion.....	7
1.2.3 THE GROWTH OF THE INTERNET AND INTERNET TRADING.....	7
1.2.3.1 Internet Growth.....	7
1.2.3.2 The Concerns and Opportunities for Businesses.....	9
1.2.3.3 Conclusion.....	11
1.2.4 ELECTRONIC COMMERCE (EC).....	11
1.2.4.1 What is Electronic Commerce?.....	11
1.2.4.2 EC Concerns and Payment Methods.....	13
1.2.4.3 Internet payment security.....	14
1.2.4.4 EC Importance Worldwide.....	15
1.2.4.5 Conclusion.....	16
1.2.5 ELECTRONIC COMMERCE AND THE IS AUDITOR.....	17
1.3 PROBLEM STATEMENT.....	19
1.3.1 RESEARCH OBJECTIVES.....	19
1.4 LITERATURE REVIEW.....	20
1.4.1 STANDARDS AND GUIDELINES.....	20
1.4.1.1 Conclusion.....	23
1.4.2 WEB ASSURANCE SERVICES.....	23
1.5 RESEARCH DESIGN.....	25
1.6 NATURE AND FORM OF THE RESULTS: DELIVERABLES.....	25
1.7 FACILITIES AND SPECIAL RESOURCES.....	26
<b>CHAPTER 2 .....</b>	<b>27</b>
<b>THE ROLE OF THE AUDITOR DEFINED.....</b>	<b>27</b>
2.1 INTRODUCTION.....	28
2.2 AUDITING DEFINED.....	28
2.3 AUDITOR TYPES.....	30
2.3.1 EXTERNAL/INDEPENDENT AUDITING.....	30
2.3.1.1 The Role of the External Auditor.....	31
2.3.1.2 General Financial Audit Objectives.....	32
2.3.2 INTERNAL AUDITING.....	33
2.3.2.1 The Role of the Internal Auditor.....	34
2.3.3 INFORMATION SYSTEMS (IS) AUDITING.....	37
2.3.3.1 Introduction – IS Auditing Defined.....	37
2.3.3.2 Information Systems Audit Control Objectives.....	40
2.3.3.3 Information Systems Audit Objectives.....	41



2.4	IS AUDIT AND MANAGEMENT EXPECTATIONS.....	42
2.5	THE CHANGING IS AUDIT ENVIRONMENT AND AUDIT OBJECTIVES.....	46
2.5.1	Auditors in an EC Environment.....	48
2.5.2	Audit Guidance in Electronic Commerce Environments.....	50
2.5.2.1	Audit Guidance Statement – AGS 1056.....	50
2.5.2.2	Web Assurance Framework.....	51
2.5.2.3	Audit Standards.....	52
2.6	THE AUDIT PROCESS.....	53
2.7	CONCLUSION.....	53
<b>CHAPTER 3 .....</b>		<b>55</b>
<b>ELECTRONIC COMMERCE AND ELECTRONIC COMMERCE PAYMENTS....</b>		<b>55</b>
3.1	INTRODUCTION.....	56
3.2	ELECTRONIC COMMERCE.....	57
3.2.1	ELECTRONIC COMMERCE DEFINED.....	57
3.2.2	THE HISTORY OF ELECTRONIC COMMERCE (EC).....	58
3.2.3	ELECTRONIC COMMERCE IN THE MARKET.....	61
3.2.4	ELECTRONIC COMMERCE CATEGORIES.....	62
3.2.4.1	B2C and B2B EC Categories.....	63
3.2.4.2	B2B Electronic Commerce.....	64
3.2.4.3	B2C Electronic Commerce.....	65
3.2.5	ELECTRONIC COMMERCE PAYMENT SYSTEMS.....	66
3.2.5.1	Online Payment Risks.....	67
3.2.5.2	Internet Payment Security.....	68
3.2.5.3	Non-Credit Card Approaches.....	69
3.2.5.4	Other Non-Credit Card Approaches.....	72
3.3	CONTROL MECHANISMS.....	74
3.3.1	ENCRYPTION.....	74
3.3.2	AUTHENTICATION.....	75
3.3.3	ACCESS CONTROL.....	75
3.4	CONCLUSION.....	76
<b>CHAPTER 4 .....</b>		<b>77</b>
<b>RISKS IN E-COMMERCE PAYMENT SECURITY.....</b>		<b>77</b>
4.1	INTRODUCTION.....	78
4.2	SECURITY AND E-COMMERCE (EC).....	79
4.3	THE SECURITY IMPLICATIONS OF THE INTERNET AS AN OPEN NETWORK.....	80
4.4	INTERNET SECURITY - THREATS AND CONCERNS.....	83
4.4.1	THE NEED FOR INTERNET SECURITY.....	83
4.4.2	BACKGROUND TO INTERNET SECURITY RISKS.....	85
4.4.3	A DEFINITION OF RISK.....	86
4.4.4	THREATS IN ELECTRONIC COMMERCE PAYMENT SECURITY.....	87
4.4.4.1	Unauthorised Access.....	88
4.4.4.2	Data Alteration/Integrity.....	88
4.4.4.3	Breach of Confidentiality Including Spoofing, Data Theft, and Fraud.....	89

University of Pretoria etd – Bezuidenhout, P S (2006)

4.4.4.4	Denial of Service/Availability.....	90
4.4.4.5	Repudiation.....	90
4.4.4.6	Client side and web side vulnerabilities.....	91
4.4.4.7	Authentication.....	92
4.4.5	RISKS RELATED TO SPECIFIC INTERNET PAYMENT METHODS.....	92
4.4.5.1	Credit Card Transactions.....	92
4.4.5.2	Electronic Cash.....	93
4.4.6	MANAGING THE RISK.....	94
4.5	CONCLUSION.....	95

**CHAPTER 5 ..... 97**

**CONTROL IDENTIFICATION FOR E-COMMERCE PAYMENT SECURITY..... 97**

5.1	INTRODUCTION.....	98
5.2	CONTROLS DEFINITION.....	99
5.3	ELECTRONIC COMMERCE CONTROLS BY RISK AREA.....	102
5.3.1	INTERNET SECURITY ISSUES - PRIVACY AND CONFIDENTIALITY.....	102
5.3.2	INTEGRITY.....	103
5.3.3	ACCESS CONTROL AND AUTHORISATION.....	103
5.3.4	NON-REPUDIATION.....	105
5.3.5	AVAILABILITY – DENIAL OF SERVICE (DoS).....	106
5.3.6	AUTHENTICATION.....	109
5.4	TECHNOLOGIES USED FOR CONTROL PURPOSES.....	111
5.4.1	ENCRYPTION AND SECURE PROTOCOLS.....	111
5.4.1.1	Encryption.....	111
5.4.1.2	Secure Protocols.....	114
5.4.1.2.1	Secure Sockets Layer (SSL).....	116
5.4.1.2.2	Secure Payment Protocols.....	119
5.4.2	PUBLIC KEY INFRASTRUCTURE.....	126
5.4.3	DIGITAL CERTIFICATION.....	132
5.4.3.1	Certification Authority (CA).....	135
5.4.3.1.1	Key Recovery/Escrow.....	139
5.4.4	FIREWALLS.....	141
5.4.4.1	Proxy Server.....	142
5.4.4.2	Packet Filter/Screening Router.....	142
5.4.4.3	Application Gateway/Dynamic Packet Filter.....	143
5.4.5	INTRUSION DETECTION SYSTEMS (IDS).....	145
5.4.6	VIRTUAL PRIVATE NETWORKS (VPN).....	148
5.4.7	CLIENT-SIDE AND WEB SERVER VULNERABILITIES.....	149
5.4.7.1	Policies.....	150
5.4.7.2	Physical Security.....	151
5.4.7.3	Server Controls.....	152
5.5	CONCLUSION.....	157

**CHAPTER 6 ..... 159**

**AN AUDIT APPROACH TO E-COMMERCE PAYMENT SECURITY..... 159**

6.1	INTRODUCTION.....	160
6.2	AUDIT APPROACH.....	161



	University of Pretoria etd – Bezuidenhout, P S (2006)		
6.2.1	A DEFINITION OF AUDIT APPROACH.....		161
6.2.2	ELEMENTS OF AN AUDIT APPROACH.....		161
	6.2.2.1 Audit Approaches from Major Accounting Firms.....		161
	6.2.2.1.1 Summary of the Audit Approaches of the Major Accounting Firms.....		162
	6.2.2.2 Audit Approaches as Prescribed by Professional Organisations.....		164
	6.2.2.3 Audit Approaches followed by Other Organisations.....		165
6.3	COMMON STEPS IN THE EC PAYMENT SECURITY AUDIT APPROACH.....		167
6.4	CONSIDERATIONS ON AUDIT PROCEDURES FOR AN EC PAYMENT SECURITY AUDIT.....		167
6.4.1	STEP 1 SCOPE AND UNDERSTAND THE ENVIRONMENT - BACKGROUND INFORMATION GATHERING.....		167
	6.4.1.1 The Results of Previous Audit Procedures.....		167
	6.4.1.1.1 General IT Environment Information Gathering.....		170
	6.4.1.1.2 EC Specific Information Gathering Considerations.....		170
	6.4.1.1.3 Legal Considerations.....		170
	6.4.1.1.4 Special Rules.....		171
6.4.2	STEP 2 RISK ANALYSIS CONSIDERATIONS.....		172
	6.4.2.1 Results of Previous Audit Procedures.....		173
	6.4.2.2 Risk Considerations for EC Payment Security.....		173
6.4.3	STEP 3 CONTROL CONSIDERATIONS.....		174
	6.4.3.1 The Nature of the Audit Procedures.....		176
	6.4.3.2 General Control Considerations.....		177
	6.4.3.2.1 Security policy, Corporate Information Security (CIS) and Security Administration.....		177
	6.4.3.2.2 Physical and Environmental Security.....		178
	6.4.3.2.3 Operating System and Web Server Considerations.....		179
	6.4.3.2.4 Change Management.....		179
	6.4.3.2.5 Business Continuity Planning (BCP).....		179
	6.4.3.2.6 Organisational Structure.....		179
	6.4.3.2.7 Computer Operations and Backup.....		180
	6.4.3.2.8 Legal Compliance.....		180
	6.4.3.2.9 Event Journal.....		180
	6.4.3.2 EC Specific Technical Security Control Considerations.....		181
	6.4.3.2.1 Firewall and Router Considerations.....		181
	6.4.3.2.2 Encryption, Privacy, and Secure Protocols.....		182
	6.4.3.2.3 Public Key Infrastructure (PKI) Considerations.....		182
	6.4.3.2.4 Intrusion Detection.....		184
	6.4.3.2.5 Virtual Private Networks (VPN) Considerations.....		184
6.5	CONCLUSION.....		185
6.6	FORMULATING THE AUDIT APPROACH FOR THE IS AUDITOR: AN OVERVIEW.....		186
6.7	THE ROLE OF THE IS AUDITOR: FINAL OBSERVATIONS.....		189

**LIST OF APPENDICES**

APPENDIX A	THE NATURE OF AUDIT PROCEDURES IN AN EC PAYMENT SECURITY AUDIT .....	193
APPENDIX B	GLOSSARY OF TERMS.....	254
<b>REFERENCES.....</b>		<b>269</b>
<b>SUMMARY.....</b>		<b>287</b>
<b>OPSOMMING.....</b>		<b>289</b>

**LIST OF TABLES USED**

Table 4.1	The Average Loss of Various Security Attacks.....	80
Table 6.1	Risk/Control Matrix.....	175
Table 6.2	Risk/Control Matrix for EC Payment Security.....	189
Table A1	IT Information to be Obtained.....	195
Table A2	Hardware Platform Configuration Information to be Obtained.....	196
Table A3	IT Installation Information to be Collected.....	196
Table A4	EC Application System Information.....	196
Table A5	General EC Application Information to be Obtained.....	197
Table A6	EC Specific Application System Information to be Obtained.....	197



## Summary

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

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

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

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

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

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

*Title: 'n Ouderskoetsing van die veiligheid van die elektroniese betalingstelsels met 'n opeenvolgende en*

*Elektroniese handel (EH) is 'n groeiende handelsomgewing en is veral van belang vir die sukses van die groeiende omgewing. Dit beteken dat die EH-omgewing 'n nuwe wêreld van risiko's en nuwe veiligheids bedreigings met 'n nuwe omgewing van goedskeuringe en keuses. Dit beteken ook dat die EH-omgewing 'n nuwe wêreld van risiko's en nuwe veiligheids bedreigings met 'n nuwe omgewing van goedskeuringe en keuses. Dit beteken ook dat die EH-omgewing 'n nuwe wêreld van risiko's en nuwe veiligheids bedreigings met 'n nuwe omgewing van goedskeuringe en keuses.*

*In hierdie studie word die volgende doelwitte aanvaar: om 'n raamwerk te ontwikkel vir die toetsing van die veiligheid van die elektroniese betalingstelsels met 'n opeenvolgende en*

- Versameling van agtergrondinligting in verband met EH-omgewing
- Identifisering van die risiko's in die omgewing
- Identifisering van moontlike kontroles wat die risiko's sal mitigeer
- 'n Opeenvolgende raamwerk vir die toetsing van die veiligheid van die elektroniese betalingstelsels met 'n opeenvolgende en

*Hierdie studie bevestig die feit dat IS-auditore hielik verantwoordelik is vir die sukses van die elektroniese handel. Dit beteken dat die IS-auditore hielik verantwoordelik is vir die sukses van die elektroniese handel. Dit beteken dat die IS-auditore hielik verantwoordelik is vir die sukses van die elektroniese handel.*

## Opsomming

Kandidaat: Pieter Stefan Bezuidenhout

Studieleier: Prof. Dr. J.D. Gloeck

Departement: Ouditkunde

Graad: Magister Commercii (Rekenaarouditering)

Titel: 'n Ouditbenadering van die inligtingstelselouditeur in 'n elektroniese handel omgewing met klem op internetbetalingsekuriteit

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

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

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

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



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

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