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

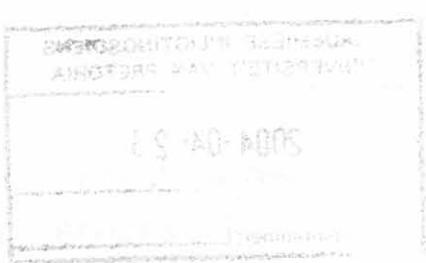
BY

PIETER STEFAN BEZUIDENHOUT

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

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

OCTOBER 2002



Foreword

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

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

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

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

NEW YORK
14 October 2002.

Contents

LIST OF APPENDICES

LIST OF TABLES USED

Summary

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

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

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

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

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

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

Opsomming

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

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

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

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

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

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

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