Amman Arab University

For Graduate Studies

The Impact of Information Technology on the Internal Audit Process in Jordan (Case Study)

By

Tala G. Al-Jabari

Supervisor

Prof. Dr. Naim Dahmash

Submitted in Partial Fulfillment of the Requirements for the Degree of Masters in Accounting

Faculty of Managerial and Financial Graduate Studies

Amman Arab University for Graduate Studies

2004

This thesis was successfully defended and approved on

Examination Committee	Signature
Prof. Dr. Naim Dahmash	
Dr. Hadi Al-Tamimi	
Dr. Nezam Hussain	

I would like to dedicate this to my loving parents

Ghazi and Laila,

My supporting brother Saif,

My encouraging friend Tala.

Acknowledgement

In preparing this study I have received valuable assistance from a number of individuals. It is a pleasure to express now my warm appreciation to each one for their time and efforts. First of all I would like to thank my supervisor Professor Naim Dahmash for his supporting and perceptive suggestions that led to elimination of numerous errors and inconsistencies.

I would like to thank the auditing team in Fastlink Company who helped me a lot in getting this study done by offering me the data I needed, and most of all by offering me their valuable time, I'm really grateful for that.

Finally, and most important, I thank my family for their assistant supporting, and encouragement.

Table of Contents

Acknowledgement III
Table of Contents..... IV
List of Tables and Flowcharts..... VII
Abstract..... IX
Arabic summary XI
Chapter one study introduction:.....1
1.1. Introduction 2
1-2 Problem Definition:.....4
1-3 Importance of the Research.....4
1-4 Research Objectives (Purpose): 5
1-5 Research Design:.....7
1-6 Previous Studies (Literature Review): 8
CHAPTER TWO Materiality, Risk, and Risk Assessment.....14
Chapter three internal control 15
3-1 Introduction.....16
3-2 Definition of Internal Control 17
3-3 Internal Audit 19
3-4 Scope of Internal Control.....20
3-5 Objectives of Internal Control 22
3-6 Inherent Limitations of Internal Control.....24
3-7 Components of Internal Control 25
3-7-1 Control Environment 26
3-7-2 Risk Assessment 27
3-7-3 Information and Communication.....29
3-7-4 Control Activities.....31

3-7-5 Monitoring 34
Chapter Four: Introduction 36
4-1 Introduction 36
4-2 How Information Technologies Enhance Internal Control 39
4-3 Risks of Information Technology 42
4-3-1 Reliance on Functioning of Hardware and Software 45
4-3-2 Visibility of the Audit Trail 46
4-3-3 Reduced Human Involvement 47
4-3-4 Systematic Versus Human Error 48
4-3-5 Unauthorized Access 48
4-3-6 Loss of Data 49
4-3-7 Reduced Segregation of Duties 49
4-3-8 Lack of Traditional Authorization 50
4-3-9 Need for IT Experience 50
4-4 Internal Controls in an IT Environment 51
4-4-1 General Controls 51
4-4-2 Application controls 59
4-5 SAS no. 94 62
Chapter five Research Methodology 66
5-1 Research Methodology and Data Gathering: 66
5-2 The Statistical Population: 67
5-3 The Difficulties of the Study: 67
5-4 Findings: 68
5-4,1 Preliminary risk assessment: 69

5-4,2 Audit Risk Analysis Model:.....70
5-5 Conclusions and Recommendations: 85
REFERENCES 89
Appendices.....93

List of Tables and Flowcharts

Table Number	*Title*	Page
5-1	IS Audit Model	78

List of Figures

Figure Number	Figure Title	Page
1	Retail Sales Process: (Risk Assessment)	81
2	Retail Sales RSS (Point of Sales) system related controls. (Risk Assessment).	82
3	Retail Sales Process: (Control Assessment).	83
4	Retail Sales RSS (Point of Sales) system related controls. (Control Assessment).	84
5	Retail Sales Process: (Risk Exposure.	85
6	Retail Sales RSS (Point of Sales) system related controls. (Risk Exposure).	86

The Impact of Information Technology on the Audit Process in Jordan (Case Study)

By
Tala G. Al-Jabari

Supervisor
Prof. Dr. Naim Dahmash

This study aims to:

Abstract

1. Discuss the nature of internal controls by focusing on the importance of internal controls for both the management and the auditor, the components of internal control systems, describe the requirements of understanding internal control, assess control risk, and describe the process of designing and performing tests of controls.
2. Determine how computer systems operate, because a practicing auditor must understand his company's computerized accounting system in depth.
3. Identify the auditor's use of computers (Auditing through the computer).
4. Determine how information technologies enhance internal controls.

5. Identify risks associated with the use of information technology.
6. Explain how specific types of general controls and application controls reduce risk associated with using IT-based accounting systems.
7. Conclude a model for auditing computerized accounting systems.

To achieve the previous objectives, the researcher conducted interviews in the auditing department in Fastlink Company, which includes ten auditors; some fieldwork and observation also took place in this study.

By conducting the above an Information System Audit Model (IS Audit Model) has been concluded. In this model it is important to begin the audit with the riskiest process or the one with highest exposure, because if these risks occur it may cause catastrophic losses for the company, in addition this model has proved its effectiveness in saving time and cost.

Hope this study achieves its objectives, and enhances the accounting and auditing profession in Jordan.

آثر تكنولوجيا المعلوماتعلىعملية التدقيق في الاردن (دراسة حالة)

إعداد

تالا غازي الجعبري

إشراف

الاستاذ الدكتور نعيم دهمش

Arabic summary

تهدف هذه الدراسة الى ما يلي:

1. مناقشة طبيعة نظم الرقابة الداخلية من خلال التركيز على أمور منها أهمية هذه النظم ومكوناتها، متطلبات فهمها و عملية تصميم و اداء اختبارات نظم الرقابة (Tests of Controls).
2. تعريف كيفية عمل نظم المعلومات الالكترونية، لأن من الأهمية أن يفهم المدقق الداخلي كيفية عمل و معالجة هذه النظم داخل الشركة التي يعمل بها.
3. كيفية استخدام الحاسوب في دعم عملية التدقيق.
4. تعزيز نظم الرقابة الداخلية باستخدام الحاسوب (Information Technology).
5. مناقشة المخاطر المترتبة على نظم الرقابة الداخلية نتيجة لاستخدام الحاسوب.
6. مناقشة و تحديد الاجراءات الرقابية التي تحد من هذه المخاطر.
7. وضع نموذج او خطوات من أجل القيام بعملية تدقيق فعلية في ظل نظام محاسبي يعتمد على الحاسوب (Information System Auditing Model).

و لتحقيق هذه الاهداف قامت الباحثة بإجراء مقابلات مع المدققين الداخليين لدى شركة فاست لينك، حيث تم اجراء هذه المقابلات مع كافة المدققين و الذي يبلغ عددهم عشرة مدققين. اضافة الى ذلك تم استخدام اسلوب الرقابة و العمل الميداني لغايات جمع المعلومات.

و نتيجة لما تم جمعه من معلومات تم التوصل الى وضع نموذج للقيام بعملية تدقيق ضمن نظام محاسبي الكتروني حيث اثبت هذا النموذج فعاليته من حيث الوقت المستغرق و تخفيض الخسائر لأنه يبدأ بالمخاطر ذات الاهمية القصوى و بالتالي تفادي خطر مثل هذه المخاطر لأنها في حال وقوعها، و عدم تفاديها في بداية التدقيق من خلال وضع أنظمة رقابية لها قد تؤدي الى وقوع خسائر كبيرة ذات آثر على الشركة.

و انطلاقا من هذا كله فأننا نأمل ان تكون نتائج هذه الدراسة قد حققت الاهداف المرجوه، من خلال المساهمة في تحسين مهنة التدقيق في الاردن.

Chapter one

study introduction:

1-1 Introduction

1-2 Problem Definition

1-3 Importance of the Research

1-4 Research Objectives

1-5 Research Design

1-6 Previous Studies

Chapter One

1.1. Introduction

With the seemingly unending innovations in information technology, resulting in higher capacities and lower costs of computers, all business organizations-large or small-are increasingly using computers for data processing (often referred to as electronic data processing, or EDP).

Computerization significantly affects the organization controls, flow of documents, and manner of information processing. As such, the approach and techniques to be followed by an auditor in IS auditing (e.g. the accounts processed on computers) are in certain respects different from those to be followed in a manual environment.

The company's integration of information technology (IT) into the accounting system affects risk and internal control. The use of IT can enhance internal control by adding new control procedures performed by the computer and by replacing manual controls subject to human error.

Although enhancing internal control, reliance on IT can introduce new risks, which the organization can manage through the implementation of controls specific to IT environment.

Auditors must be careful in assessing control when the organization has technology-based accounting systems before they can accept the reliability of any computer-generated output. A common assumption is that the information is correct because the computer produced it. Too often, reliance is placed on the untested accuracy of computer-generated output because auditors fail to remember that computers perform only what they are programmed to do. Auditors must understand and test computer-based controls before concluding that computer-generated information is reliable.

This research highlights risks specific to IT environment by studying how to assess risk and developing a module for risk assessment, and then identify controls that can be implemented to address those risks.

1-2 Problem Definition:

The problem definition is going to be set in the form of a research question. The audit division management objectives in Fastlink will be taken into consideration as follows:

- What are the risks associated with the application of information systems and how are these risks assessed (Audit Risk Model)?
- What are the controls applied in order to overcome these risks?
- What are the steps to perform an IS Audit in companies that depend on information systems (taken Fastlink as a case study)?

1-3 Importance of the Research

The application of Information Technology in Auditing in Jordan still lacks a thorough understanding. This study takes a close look at the system used by Fastlink Company, which was chosen because of the large size of it's customer base and the complexity of it's operations. The study aims to reflect Fastlink's experience with such systems, their efficiency, the dangers associated and if whether or not these dangers outweighed the benefits of Electronic Data Processing systems (EDP). Also, the study will introduce the actions taken to overcome the flaws in the system, if any.

1-4 Research Objectives (Purpose):

The general purpose of this study is to determine the impact of information technology on the audit process in the client's organization and the auditor's firm, and how information technologies enhance internal controls, and the risks associated with the use of information technologies in the client's organization.

In order to implement this study a closer look on the subject "Internal Controls in the client's organization" must be taken.

These concepts will be applied in Fastlink Company, one of Jordan's service companies due to its large financial department that contains systematic internal controls and are heavily dependent on information technologies.

A careful review of the problem's questions led to the development of the following specific research objectives:

1. Discuss the nature of Internal Controls by focusing on the following:

- The importance of Internal Controls for both the management and the auditor.

- The five components of Internal Control Systems.
  a) Control environment.
  b) Risk assessment.
  c) Control Activities.
  d) Information and communication.
  e) Monitoring.[1]
- Describe the requirements of understanding Internal Control and assessing control risk.
- Assess control risk by linking strengths and weaknesses of Internal Control to transaction-related audit objectives.
- Describe the process of designing and performing tests of controls.

2. To determine how computer systems operate, because an internal auditor must understand his company's computerized accounting system in depth.
3. Identify the internal auditor's use of computers (Auditing through the computer): Describe the use of Test Data, Parallel Simulation, and Embedded audit Module approaches when auditing through the computer.

[1] A. Arens, and J. Loebbecke *Auditing: An Integrated Approach*, 8th ed. Upper Saddle River, NJ.: Prentice Hall, 2000, p. 292.

4. Determine how information technologies enhance internal controls.
5. Identify risks associated with the use of information technology.
6. Explain how specific types of general controls and application controls reduce risks associated with using IT-based accounting systems.
7. Conclude a Model for Information Technology Auditing (IS Auditing).

1-5 Research Design:

Case study will be the exploratory research technique; the survey will be the basic data gathering method (Research Design). Each internal auditor of Fastlink's company will be interviewed. Each respondent will be interviewed in his office. The personal interviews are generally expected to last approximately one hour.

A verity or types of research questions will be asked, some will be open ended response questions, others will be fixed-alternative questions.

A couple of sample questions that will be asked are:

- What are the controls implemented to address many of the risks associated with the reliance on IT?
- How often do you evaluate these internal controls?
- In what capacity did computer controls replace manual controls:

1. Partially.
2. Fully.

Also some fieldwork and observation will take place in this research.

Since the study will be applied to Fastlink Company the interviews will be made with all internal auditors, which are 10 auditors, so there will be no sample, the study will be based on census.

No hypotheses (Null hypotheses or alternative hypotheses) will be presented in this study since there is no correlation to be established; instead this research will produce a module in risk assessment and controls concerning IS auditing.

Data Gathering:

The researcher will personally conduct the interviews.

Data Processing and Analysis:

Standard editing and coding will be utilized.

Simple tabulation will be utilized to analyze data.

1-6 Previous Studies (Literature Review):

- In a study done by Walton and Vittori (1983) they concluded that the impacts of Information

- Technologies could be dynamic and reciprocal. Not only can IT directly affect roles and behavior, but the users of IT can develop ways of using IT which can produce their own second order effects on both managers and subordinates.[2]
- *"The use of Information Technology in the audit process: illustrations from two big audit firms"* is the title of a study done by Stuart Manson and others in July 1997 which explores the use of Information Technology for audit automation purposes in two big audit firms.[3]

This study has provided support for seeing Information Technology in the knowledge- based organization as replete with ambiguity and duality, and hence for a structuration approach to understanding the interaction between Information Technology, culture and organization.

- In a study done by Dillard and Bricher (1992) recognized that knowledge-based systems might be able to reduce costs and increase audit quality in the short term. They argued, however, that there is a

[2] Manson, S., Mccartney, S. and Sherer, M., "*The use of Information Technology in the audit process: illustration from two big audit firms"* Paper Presented at the Department of Accounting and Finance and Management, University of Essex, July 1997.

[3] Ibid.

- danger that necessary human development and expertise will be sacrificed if high-level decisions and judgements routinely come within the domain of such systems. [4]
- In a recent study done by the General Accounting Office (GAO) titled *E-filing security* (2001) which is the most modern way to submit the taxpayers tax returns, found that many of the IRS security controls were inadequate.

In the study, they discovered and demonstrated that hackers could have gotten into the system and retrieved confidential tax information quite easily and in 2000 five major problems with E-filing were discovered and the GAO made a list of recommendations for the IRS technical staff to review.[5]

- The AICPA conducted a survey to assess the current information security issues that accountants feared most.

The survey results were divided into two parts, the first part covered the CPA's top concerns for Audit Information

[4] For more information visit *www.odu.edu.com.*
[5] For more information visit *www.ISACA.com.*

Systems (AIS) that come with new and updated technology. The second part talked about several perks that benefit accountants from the use of new technologies.[6]

- In a recent study entitled *IS Auditing* done by G. Randolph Just and Michael P. Fabrizius, CIA, CPA 2000[7], managing and controlling the effect of change resulting from new technologies and the effectiveness of organizations' internal business controls was discussed. This study was applied in the health care industry.

This study is still developing and the researchers haven't documented the final results yet.

- Enterprise Information Integrity Project is a project recently done by the Information Systems Audit and Control Association (ISACA).The Centre for IS Assurance is slated to conduct this project for the Information Systems Audit and Control Foundation (ISACF) with funding from Unitech Systems Inc. The purpose of this project is to define the key elements of Enterprise Information Integrity,

[6] For more information visit *www.AICPA.com.*
[7] Tucker, George, H., *"IT and the Audit"* The Journal of Accountancy, Academic Search Elite, 2000.

- as well as benefits criteria associated with them and present a framework and process for management. In an increasingly dynamic
- global environment, IT organizations must address complex solutions and operating environments to provide assurance of the dependability and trustworthiness of information across the enterprise.[8]

Recent Projects:

- "Security, Audit and Control Features Security and Audit Principles (SAP)" is the name of a Technical and risk Management Reference Guide; this guide is one of the ISACA recent projects.Current best practices and future trends in Electronic Data Processing (EDP) issues are documented in a practical how-to guide to enable auditors and risk professionals (IT and non-IT) to evaluate risks and controls in existing EDP implementations and to facilitate the design and building of better practice controls into system upgrades and enhancements.

SAP is one of the leading developers of enterprise applications worldwide. Its primary EDP product is SAP R/3. This guide covers SAP R/3 and includes the following topics:

[8] For more information visit www.ISACA.org.

- Major SAP R/3 modules, products and functionality and navigation guidance
    - Strategic risk management in an EDP environment to minimize the risk of not obtaining the significant benefits that can flow from a well-executed EDP implementation
    - EDP audit impacts from implementation; frameworks and methodologies for auditing and testing in an SAP R/3 environment.
    - Auditing SAP R/3 core business cycles: revenue, inventory and expenditure. Risks and automated controls are outlined and sample testing techniques are suggested.
    - Auditing SAP R/3 Basis technical infrastructure. Specific risks in SAP R/3 security and control, automated control activities and sample assurance techniques are provided.
    - New directions for SAP R/3 Audit. SAP solutions for e-business.

CHAPTER TWO

Materiality, Risk, and Risk Assessment

2-1 Introduction

2-2 Materiality

2-3 Audit Risk

2-4 Types of Risks

2-5 Risks of Information Technology

(This chapter is missing in the English source)

Chapter three
internal control

3-1 Introduction

3-2 Definition of Internal Control

3-3 Internal Audit

3-4 Scope of Internal Control

3-5 Objectives of Internal Control

3-6 Inherent Limitations of Internal Control

3-7 Components of Internal Control

Chapter Three

3-1 Introduction

Effective internal controls are the foundation of safe and sound business. A properly designed and consistently enforced system of operational and financial internal control helps an organization's board of directors and management safeguard its resources, produce reliable financial reports, and comply with laws and regulations. Effective internal control also reduces the possibility of significant errors and irregularities and assists in their timely detection when they do occur.

An Entity's board of directors and senior management cannot delegate their responsibilities for establishing, maintaining, and operating an effective system of internal control. The board must ensure that senior management regularly verifies the integrity of the organization’s internal control.

Although internal control and internal audit are closely related, they are distinct from each other. Internal control is the systems, policies, procedures, and processes effected by the board of directors, management, and other personnel to safeguard business assets, limit or control risks, and achieve

the organization's objectives. Internal audit provides an objective, independent review of activities, internal controls, and management information systems to help the board and management monitor and evaluate internal control adequacy and effectiveness.

3-2 Definition of Internal Control

Internal control is an essential prerequisite for efficient and effective management of any organization. It is, thus, a primary responsibility of every management to establish and maintain an adequate system of internal control appropriate to the size and nature of the business of the entity.

Security and Audit Principles, Principle 6 (SAP 6) defines the system of internal control as:

"The plan of organization and all the methods and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring, as far practicable, the orderly and efficient conduct of its business, including adherence to management policies,

the safeguarding of assets, prevention and deduction of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable

financial information. The system of internal control extends beyond those matters which relate directly to the functions of the accounting system."[9]

A more conventional definition of internal control is that proposed by the Committee of Sponsoring Organizations (COSO) and reads as follows:

"Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Reliability of financial reporting.
- Compliance with applicable laws and regulations.
- Effectiveness and efficiency of operations."

[9] FASB, "Qualitative Characteristics of Accounting, *"Statement of Financial Accounting Concepts No. 2.* Stamford, Conn.: Financial Accounting Standards Board, 1980, p. xv.
[9]

3-3 Internal Audit

Internal auditing is:

"An independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization."[10]

The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analysis, appraisals, recommendations, council and information concerning the activities reviewed.[11]

Management determines the scope of internal audit. For example, the scope of internal audit in an enterprise may be confined to reviewing whether the accounting and allied records have been properly maintained, the assets of the enterprise adequately safeguarded, and the policies and procedures laid down by the management complied with.

[10] D. Taylor and G. Glezen. op. cit. p. 5.
[11] H. Beverly, "Technology and Management Control Systems", Accounting, Management and Informatrion Technology, Vol. 3, No. 3, 1993, pp. 151-171.

On the other hand, the scope of internal audit in an organization may be wide enough to include a review of whether the resource-utilization in the enterprise is efficient and effective. In any case, internal audit is essentially a post-transaction review to evaluate the records, controls, and operations in an organization, which serves as a self appraisal process.

3-4 Scope of Internal Control

As illustrated previously, in the COSO definition of internal control, the main objectives of internal control (reliability of financial reporting, compliance with applicable laws and regulations, and effectiveness and efficiency of operations) the scope of internal control extends beyond issues of accuracy of financial statements. Hence, not all objectives of internal control are relevant to an audit process. Internal audits may be considered a subordinate category of the internal control structure of an organization.

For example, an internal control structure, aiming to fulfill the objectives of internal control would generally also include operational controls and administrative controls such as quality control, work standards, budgetary control, periodic reporting, policy appraisals, quantitative controls, etc., all being parts of the internal control system.

In an independent financial audit, auditors are primarily concerned with controls relevant to financial statements, since these have a direct and significant bearing on the reliability of financial information.

Administrative controls, on the other hand, have only an indirect relationship with financial records and the

auditor may evaluate only those administrative controls which have a bearing on the reliability of financial records. Thus, an auditor of financial information may not normally be interested in evaluating the system for getting the production manager's approval of the samples of a manufactured product.

3-5 Objectives of Internal Control

Control systems can help managers measure performance, make decisions, evaluate processes, and limit risks. Good internal control can help an organization achieve its objectives and avoid surprises. Effective control systems may detect mistakes caused by personal distraction, carelessness, fatigue, errors in judgment, or unclear instructions in addition to fraud or deliberate noncompliance with policies. Effective and well-designed control systems are still subject to execution risk. In other words, human beings still must execute most control systems and even well trained personnel with the best of intentions can become distracted, careless, tired, or confused.

In accordance with the COSO definition of internal control, an internal control system or structure within an organization is primarily the responsibility of the

board of directors of the organization, keeping in view the requirements that are specific to the organization, e.g. nature of business, volume of operations, degree of professionalism of management, etc. In general, and in addition to the objectives set forth in the COSO definition, the objectives of an internal control system, according to the Security and Audit Principles 6 (SAP 6), would include:

1. The transactions are executed in accordance with the management's authorization.
2. All transactions are promptly recorded in an appropriate manor to permit the preparation of financial information and to maintain accountability for assets.
3. Assets are safeguarded from unauthorized access, use or disposition.
4. Assets are very verified at reasonable intervals and appropriate action is taken with regard to discrepancies.[12]

[12] K. Gupta. Op. cit. p. 83.

3-6 Inherent Limitations of Internal Control

By establishing an internal control system, management of organizations can only ensure, to a certain degree, that organization goals are being fulfilled. This is due to the fact that internal controls have inherent limitations.

These limitations arise due to the following reasons:

1. Controls have to be cost-effective. Thus, some controls may not be instituted merely because they are not cost-effective.
2. Most controls are directed at transactions of a usual nature. Therefore, transactions of an unusual nature might escape being subjected to rigorous controls.
3. Human errors remain even if the internal control system was sufficiently established.
4. Any system of control has its limitations in preventing frauds through collusion between two or more persons.
5. Members of the management may themselves override the controls.

6. Controls may not keep pace with changes in conditions.
7. Management itself may manipulate transactions or estimates.[13]

3-7 Components of Internal Control

Internal control consists of five interrelated components; control environment, risk assessment, information and communication, control activities, and monitoring. Each component is integrated into the management process (i.e., planning, organizing, directing and controlling) and is essential to achieving the objectives of internal control.

The five components also serve as criteria for evaluating the effectiveness of the internal control structure. Each of these criteria must be satisfied according to the unique needs of the organization, and underlying activities, being evaluated. The fact that the components serve as both requirements and criteria is very important. This allows management to establish, maintain, and evaluate

[13] K. Gupta. Op. cit. pp. 83-84.

using the same standard. The following is a description of the five components of internal controls.

3-7-1 Control Environment

"The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all components of internal control, providing discipline and structure (AU 319.25)"[14].

The control environment is influenced by a company's history, culture and prevalent values throughout the organization, and sets the tone of the organization, influencing the control consciousness of its personnel. The control environment has a pervasive influence on the way business activities are structured, objectives established, and risks assessed. It also influences control activities, information and communication systems, and monitoring activities. Effectively controlled companies strive to have competent people, instill a company-wide attitude of integrity and control consciousness. They establish policies and

[14] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 330.

procedures, including a written code of conduct, which fosters shared values and teamwork in pursuit of the company's objectives. According to (AU 319.25), the control environment is evaluated based on the following factors:

- Integrity and ethical values
- Commitment to competence
- Board and audit committee
- Management philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practice.[15]

3-7-2 Risk Assessment

"Risk assessment for financial reporting purposes is an entity's identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented in conformity with generally accepted accounting principles (AU 319.28)".[16]

[15] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 330.
[16] Ibid. p. 333.

All organizations regardless of size, structure, nature, or industry, encounter risks at all levels within their organization. Risks affect each company's ability to survive, successfully compete within its industry,

maintain financial strength and positive public image, and maintain the overall quality of its products, services, and people. There is no practical way to reduce risk to zero. Indeed, the decision to be in business creates risk. Management must determine how much risk is to be prudently accepted, and strive to maintain risk within these levels. Objective setting is a precondition to risk assessment. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks. Objective setting, hence, is a key part of the management process. While not an internal control component, it is a prerequisite to and an enabler of internal control.

As mentioned, internal controls should generally be designed in a manor where they are aligned with organization objectives, in order to limit the risks associated with the process developed to address an organization's objectives. Hence, risk assessment is prerequisite to internal control and goes beyond the scope of producing sound financial statements. Conversely, assessment of inherent and control risks by auditors is primarily concerned with validity of information presented in financial statements.

3-7-3 Information and Communication

"The information and communication system relevant to financial reporting objectives, which includes the accounting system, consists of the methods and records established to identify, assemble, analyze, classify, record, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets and liabilities.

Communication involves providing a clear understanding of individual roles and responsibilities pertaining to internal control over financial reporting (AU 319.34)."[17]

Efficient information flow channeling involves the engineering of the human environment to improve the way knowledge is produced, shared, captured, acquired, and used within an organization for the purpose of providing the right information to the right people at the right time to make and take the right decision.

A firm understanding of an organization's objectives throughout the organization is key to efficient internal control. This involves personnel understanding their roles in the internal control system and how their roles relate to others, which enables problem recognition, solving and corrective action.

Organizations communicate with various external groups that may have an impact on the operations and activities of the department. To ensure effective external communications, management should provide

[17] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 334.

for open lines of communications with contractors, suppliers, and other customers of the agency. These groups provide significant feedback regarding the quality and design of agency business processes and supporting activities.

3-7-4 Control Activities

"Control activities are those policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities have various objectives and are applied at various organizational and functional levels (AU 319.32)."[18]

Documented policies and procedures should clearly indicate the actions and responsibilities of all employees relative to performance of job responsibilities. Management should formally approve these with regular updates on changes that may have occurred.

SAS 78 and the COSO report defined the following four categories for control activities that pertain to financial reporting:

[18] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 336.

1. Segregation of duties.
2. Information processing
3. Physical controls.
4. Performance reviews.[19]

3-7-4-1 Segregation of Duties:

Duties and responsibilities should be divided among staff to reduce the risk of errors, waste, misuse, or fraud. No one individual should control all key aspects of a transaction or event. This can be done by allocating responsibilities to more than one role in a manner where they complement one another, or by having an independent role that is to check the accuracy of work performed by another.

[19] A. Arens, and J. Loebbecke. Op. cit. p. 295.

3-7-4-2 Information Processing:

Several control activities may be used to verify data accuracy, completeness, and appropriate authorization of transactions. Control activities for information processing include procedures to ensure that: data entered into systems is subjected to edit checks and matched to approved control files, transactions are accounted for in numeric sequence, file totals are compared with control accounts, exceptions are examined and acted upon, and access to data, operating system, and program files (source and object code) is granted to only authorized individuals.

3-7-4-3 Physical Controls:

Equipment, inventories, securities, cash, and other assets vulnerable to risk of loss or unauthorized use, must be physically secured, periodically counted, and compared to amounts shown on control records.

3-7-4-4 Performance Reviews

All levels of organization management should review performance reports, analyze trends, and relate results to targeted and historical performance. The accuracy of operational

summaries should also be verified. Control activities must be established to monitor performance indicators. This control requires comparisons and assessments relating different sets of data to one another for analysis of relationships and appropriate corrective action. Management should investigate unexpected results, unusual trends, or conditions that may prevent the organization from achieving its business objectives.

3-7-5 Monitoring

"Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions (AU 319.38)."[20]

A system of internal controls; to ensure proper monitoring and assessment of activities; must be integrated into the everyday operations of an organization. To maintain ongoing assurances about the continued effectiveness of the internal control structure, management must continually monitor the system to identify the need for changes.

[20] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 347.

Although management (and internal auditors) maintains primary responsibility for monitoring the system of internal controls, non-managerial employees are also important to monitoring the system on a daily basis; they are often closest to the operations and, therefore, are in the best position to determine where processes (and related controls) can be improved.

Chapter Four:

Introduction

4-1 Introduction

The last four decades of the twentieth century witnessed the birth of the computer age. Computers have become an essential tool for nearly every corporate employee and have a tremendous effect on all aspects of human activity.

Over the past decade, technological advances in personal computers (PCs) have been taking large leaps, these advancements are accompanied with continuous drops in PC prices, and hence, use of computers is becoming a trend and a necessity in all industries. Computers now have a significant role in the processing of economic information.

Today corporations must be able to respond quickly to market pressures and must be able to analyze large quantities of data to make appropriate decisions. To be of any use to the corporation, this data must be accurate, relevant, and available immediately. Information technology has provided corporations with computer and software infrastructures that provide accurate and relevant data in a timely manner.

A thorough understanding of information technology has become mandatory for organizations, in order for them to make the right decisions and align their technological infrastructure with organizational goals. Likewise, a thorough understanding of information technology is essential for auditors, in order for them to be able to assess potential sources of risk.

In an atmosphere like this, it is critical that all auditors understand the impact of information systems on control and auditing. Today's auditors must be fully integrated auditors; understanding information systems and able to function effectively within a technical environment. This understanding is no longer the exclusive domain of the IT departments or even information systems auditors. High tech has created new roles and responsibilities for everyone in the audit function. Auditors must know what the new technologies are, the risks and exposures involved and how they affect audit plans and the audit.

Today's auditors are becoming more proactive and coactive, rather than reactive. In their broadened role, they participate with management in strengthening the overall control framework since stakeholders and regulatory agencies expect and

require organizations to be more accountable for solid internal controls and the proper and accurate disclosure of financial information.

Boards of directors and senior management are now facing the challenge of having the right resources that can properly interpret the organization's technologies and its related control implications, since some of the specific methods appropriate for implementing auditing concept change as systems become more complex taken into consideration that the generally accepted auditing standards and their interpretations remain the same.

This chapter will highlight how information technologies enhance internal controls and businesses in general, the risks associated with the implementation of information technologies, and the controls specific to information technology environment.

4-2 How Information Technologies Enhance Internal Control

Technology has increased the ability to capture, store, analyze and process tremendous amounts of data and information, technology has the potential to dramatically change organizations and business

practices, reduce costs, and create new opportunities. This has increased the empowerment of the decision maker. Even simple businesses are replacing inefficient manual accounting practices with computerized accounting systems in order to handle the increasing needs of information growth and to operate more efficiently and effectively

.

The incorporation of Information Technology didn't result only in introducing new risks; it also enhanced the businesses in general and the internal controls in specific. Some of these enhancements could be summarized as follows:

- It has impacted what can be done in business in terms of information and as a business enabler. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information, which has increased the empowerment of the business decision maker. Technology has also become a primary enabler to various production and service processes. It has become a critical component to business processes. There is a residual effect in that the increased use of failures, and increased awareness of the need for control.

- Computer controls replace manual controls:[21]
  The last decade has seen tremendous growth in information technology. Most mid to large-size companies have automated their accounting and information systems due to their ability to process tremendous volumes of transactions, and because they contain built-in controls that could limit the occurrence of errors in routine transactions since manual procedures are replaced with programmed and automated procedures that eliminates human error. Internal auditing functions have improved their control and monitoring activities; thus, providing better prevention and detection of misstatements.

- Higher quality information is available:[22]
  Based on the mentioned above the computer can process data with less routine transaction errors and contain specific controls to eliminate them, hence grant management

[21] A. Arens, and J. Loebbecke. Op. cit. p. 330.
[22] Ibid. p. 330.

with more and higher quality information to help senior and upper management in decision making.

4-3 Risks of Information Technology

Financial institutions operate in a technology intensive industry. Almost all aspects of operations are automated and most business transactions are consummated without the exchange of currency. Instead, transactions are stored, processed, and transported electronically using information systems and technology.

Financial institutions have long stored information in electronic form. Historically, however, transaction entry remained largely a manual process, providing a traditional paper trail through which the accuracy of electronically produced output reports could be verified. Today, advancements in communication technology are increasingly replacing institution-controlled, paper-documented transactions with electronic entries initiated by customers,

by telephone or PC, by merchants, through automated bill payment, etc. Financial institutions need new methods to control transaction input, to ensure its accuracy.

Furthermore, as the dependence on electronic information grows, it is increasingly important to take appropriate measures to ensure the integrity of the input, to protect against corruption of the data or the programming, and to test the accuracy of the output.

Risks are inherent in all electronic capabilities. Threats can come from both internal and external sources. Outside hackers, disgruntled employees, and inadvertent errors can adversely affect reliability. Unauthorized parties may inappropriately alter Web sites or hackers may initiate denial of service attacks to prevent customers from transacting business. Electronic mail containing confidential or proprietary information may be distributed in error. Unauthorized parties might access networked systems that are directly connected to an institution's main operations database, revealing sensitive data.

The integration of information technology in businesses in general and in accounting in specific has provided many benefits to the organization's internal control system, since many risks associated with manual procedures are eliminated. On the other hand the implementation of information technology in accounting has introduced new risks that could increase the likelihood of material misstatements in financial statements that should be taken into consideration by the auditor when assessing control risk.

Risks associated with the implementation of information systems could be summarized by the following general identified risks:

1- Reliance on functioning of hardware and software.

2- Visibility of the audit trail.

3- Reduced human involvement.

4- Systematic versus human error.

5- Unauthorized access.

6- Loss of data.

7- Reduced segregation of duties.

8- Lack of traditional authorization.

9- Need for IT experience.[23]

The following sections provide a brief description of each of the identified risks above:

4-3-1 Reliance on Functioning of Hardware and Software

This generally refers to the risks associated with physical standing of hardware and software, where specific internal controls need to be instated in order

[23] A. Arens, and J. Loebbecke. Op. cit. p. 331.

to protect hardware and software from misuse, vandalism or even environmental conditions, such as heat and humidity, that may be detrimental to an organization's computers.

For example, most organizations today rely on centralized servers for most data storage and network administration. Hence, such server machines usually hold sensitive and critical data and are required to be up and operational around the clock. This leads to heating up of computer processors and susceptibility to higher room temperatures. Organizations that sensitively handle their server machines usually keep them in special rooms that do not have windows and are equipped with devices for air conditioning that keep room temperatures and humidity at proper levels.

4-3-2 Visibility of the Audit Trail

Auditors depend on what is known as an audit trail in order to establish evidence regarding information provided in financial statements. Audit trails may constitute documents that are created as transactions are being processed and represent the succession of information leading to the account balance or financial statement.

As the use of modern software and dedicated database servers increases in the world of accounting, so does the level of abstraction of the interim processes involved in order to produce final reports, where many of these processes are automated. In fact, encapsulation of interim processes has become essential for good software engineering practice, making the gathering of evidence more difficult for the auditor.

4-3-3 Reduced Human Involvement

As mentioned above, encapsulation of interim processes has become common practice in software development. In addition to making it more difficult to establish the audit trail, this also leads to the reduced involvement of personnel in all levels of financial processes, which may lead to the difficulty of identifying potential misstatements as transactions are being recorded or processes. What makes it even more difficult is the fact that most computer output for financial reporting is usually summarized to a great degree. Additionally, personnel generally regard computer output as accurate, an assumption that is not always true considering computers only do what they are programmed to do.

4-3-4 Systematic Versus Human Error

Human error, or otherwise known as random error, is pretty much eliminated in electronic systems; processing of information is accurate with computers. However, the problem with computer processing is systematic error, which is error in the actual procedure underlying procedures generated by software. Software is developed to handle as many cases and scenarios as the analysts and programmers are able to identify when building the system. Therefore, there are conditions where certain transactions are anomalous to the system and in these situations these transaction are not processed correctly, but may be fully processed and due to the automated nature of the system, incorrect data may very well go by unnoticed.

4-3-5 Unauthorized Access

Most organizations today employ networked systems with critical data being stored in centralized locations and access to these data through employee terminals. Different roles in organizations possess different needs for data and different levels of authorization, but are all usually physically connected to same servers. Unauthorized access to an organization's resources from either personnel

without proper access permissions or external parties, such as hackers, is an issue that should be given a good deal of attention, where proper internal controls need to be instated to safeguard recourses, such as passwords, user Id's, firewalls, etc.

4-3-6 Loss of Data

Insufficient data may well be a source of misstatement in financial statements. In this respect, protection against loss of data, as a result of system crashes or hardware malfunctions, is essential to an any organization. For example, creating backups of all essential data on a daily basis may be given as one example of a practice to protect against data loss.

4-3-7 Reduced Segregation of Duties

As discussed in the previous chapter, segregation of duties has become essential practice as to enforce a form of internal control within an organization. In automated systems, most processing of financial transactions is done by the computer, resulting in having only one person responsible for the entire process, and hence, reduced segregation of duties. This makes

it more difficult for auditors and organization personnel to gather evidence pertaining to information presented in financial statements and validating summary information provided by the computer. Additionally, safeguarding organization data my be at jeopardy considering the fact that only one person is being responsible for entire processes, which renders the data susceptible to issues such as theft and inaccurate reporting.

4-3-8 Lack of Traditional Authorization

Another common practice in organizations is the requirement for proper authorization prior to taking certain actions relevant to financial reporting. In automated systems, such actions may be processed without requiring authorization, another example of reduced segregation of duties, but substantial enough to be mentioned as a separate type of risk.

4-3-9 Need for IT Experience

The complexity of IT systems is on a rise and most organizations today, even small to medium sized companies, are employing systems that require qualified personnel to install, customize, maintain, use

and update their software and hardware backbone.

Also, as the needs of an organization become more complex, so do the information systems that address these needs. This necessitates employing key personnel with backgrounds in various areas of information technology.

4-4 Internal Controls in an IT Environment

From the discussion of the risks associated with information technology, one can conclude that there exists a great need to consider these risks when developing internal controls for an organization.

Internal controls in environments that implement information technology are generally classified into two widely recognized categories; general controls and application controls, which has become the traditional classification for internal controls pertaining to information technology.

4-4-1 General Controls

Broadly speaking general control procedures provide management with overall (as opposed to specific) assurance as to the combined completeness, validity and accuracy of one or more levels of aggregation for often more than one application by providing an environment

in which specific control procedures may function effectively. For this reason, general controls are also referred to as environmental controls, as well as pervasive control plans and, in an

information technology (IT) environment, as general DP (data processing) controls. The following are five generally accepted categories of general controls:

1) Organization and operation controls
2) System development and documentation controls
3) Hardware and system software controls
4) Access controls
5) Data and procedural controls[24]

4-4-1-1 Organization and Operation Controls

These controls would generally lend themselves to trends and culture in an organization pertaining to information technology and how well procedures address strategic objectives. More importantly, these controls would address issues related to segregation of duties amongst

[24] W. Boynton; R. Johnson; and W. Kell. op. cit. p. 338.

IT department personnel, and between them and individuals from other departments. This would require defining roles and responsibilities and allocating them to more than one individual. As previously explained, segregation of duties becomes more difficult in an environment applying information technology, and

hence, segregation of duties becomes more geared towards individuals fulfilling IT functions.

4-4-1-2 System Development and Documentation Controls

These types of control are primarily concerned with the review, testing and approval of features in all organization systems, specifically new systems, and documentation of all these features that would include data flow diagrams, procedures for program changes, test results, etc. In general, all information related to computer systems and changes should be properly documented, testing should be conducted by various parties in an organization on a continuous basis, and the results should be documented in a consistent manor.

4-4-1-3 Hardware and System Software Controls

Specific controls aught to be instated in order to protect hardware resources, software resources and the integrity of data transmitted between computer terminals using software. Certain tests have become common to many organizations that help detect any hardware or software problems, such as:

Dual read, which is the process of reading data entered into a system twice, then compared, to make sure it is being properly entered.

- Parity check, which is the process of adding an additional bit to transmitted data, which would indicate at the receiving end that the entire data packets are being sent.
- Echo check, which is the process of sending data received to the sender, in order for it to be checked against the originally sent data.

- Read after write, which is the process of reading the data after it has been written to storage media or output, in order to be compared against the original for verification.[25]

4-4-1-4 Access Controls

Internal auditors are expected to know the strategic value of the data and information that is held by their organization. They must also ensure that the organization has some kind of access control or protective system that prevents unauthorized users from accessing such material.

To be truly effective, an access-control system must provide the appropriate level of protection with minimum interference to users. After all, if accessing information is difficult, users will either seek to obtain the data in an unauthorized way or create their own copy on their local hard disk, each of which introduces unnecessary risks to the organization and its data.

[25]W. Boynton; R. Johnson; and W. Kell. op. cit. p. 340.

An access-control system should also enable users to do the job they are authorized to do, but no more.

In addition to automated access and authorization controls, organizations must also establish physical security controls to prevent direct access to systems, because any attacker who can actually touch a system may be able to copy, remove, or delete information. The level of physical protection depends on the sensitivity and organizational value of the information contained within the organization's building. At a minimum, this should include locking doors and windows and setting up some form of security or reception control to vet arrivals and departures.

Most access-control systems rely on passwords. Unfortunately, many people use passwords that are easy to guess or break. Most organizations today have employed systems that require user to change their passwords at specific intervals (e.g. 3 months). Other examples would include specifying lengths for passwords, requiring the usage of combinations of letters and numbers, and no five consecutive passwords may be alike. All these practices are quite common in organizations. In fact, they have become standard operating system features, and do not require administrators to follow up on password issues, simply select the right features for user passwords.

4-4-1-5 Data and Procedural Controls

Such controls would entail proper backup and recovery schedules. Conventionally, there are three types of backup procedures: full system backups, differential backups and integral backups. At least one kind of the three should be carried out every day,

a combination of the three should be carried out on a weekly basis to ensure all organization data and variations to it have been

recorded and may be recovered at any time with minimal loss, in the event of system crashes or failures. Also, system backups may be stored in offsite locations such as banks.

Also, in some organizations, data entered into the system is verified at the point of entry and before it is to be committed to a database for processing, and processed data is checked before being recorded. These controls and procedures are organization specific and depend on how management sets strategic goals and processes to address them.

4-4-2 Application controls

These controls relate to the transactions and standing data appertaining to each computer-based application system and are therefore specific to each such application as opposed to general controls. The objectives of application controls, are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from programmed processing. Examples of application controls include data input validation, agreement of batch totals, encryption of data transmitted, etc. The following are three generally accepted categories of application controls:

1) Input Controls.

2) Processing Controls.

3) Output Controls.[26]

4-4-2-1 Input Controls

[26]A. Arens, and J. Loebbecke. Op. cit. pp. 336-337.

The first source of potential error, when considering automated systems, is that related to the input of data into the system for processing and then producing of financial statements. Hence, it becomes essential to incorporate controls that help mitigate, if not eliminate, the potential for error due to input mistakes, regardless of the complexity and accuracy of processing of the system.

The most common approach to control input errors is to require authorization prior to committing the data for processing. This is usually carried out by personnel other than those whom entered the data, resulting in segregation of duties. Also, conventional systems development today that involves serializing sensitive data to a database usually requires data validation functions at the input level.

4-4-2-2 Processing Controls

To minimize potential errors that may occur during the processing of financial data by applications, functions that have the ability to detect, avoid and even correct processing errors are embedded in the software. In IT environments, these controls are mostly enforced without the involvement of personnel, it is rather the responsibility of the application in specific to impose such controls. This is essential at the application level, despite the fact that processing errors are addresses through general controls that entail system development and documentation controls.

4-4-2-3 Output Controls

These are controls instated to test the validity of financial information after it has been processed. The following are three common examples of output control methods:

1. Reconciliation of totals, which involves a simple check of totals.

2. Comparison to source documents, which involves either printed or machine sensible files to compare source documents to output.
3. Visual scanning, which depends on an understanding and prior estimation of expected results.[27]

4-5 SAS no. 94

It is essential when talking about internal control in an IT environment to discuss the SAS no. 94.

Over the past several years the AICPA Auditing Standards Board (ASB) has given considerable attention to how IT affects audits. In April 2001 it issued SAS no. 94, "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit", which amends SAS no. 55, "Consideration of Internal Control in a Financial Statement Audit". SAS no. 94 provides guidance on the effect of IT on internal control and on the auditor's understanding of internal control and assessment of control risk.

SAS no. 94 is not intended to apply to the audits of only very large organizations with sophisticated IT systems since such technology may affect the audit

[27]W. Boynton; R. Johnson; and W. Kell. op. cit. p. 346.

of any size business, and its impact on internal control is related more to the nature and complexity of the systems in use than to the entity's size.

SAS no. 94 says an organization's IT use may affect any of the five internal control components—the control environment, risk assessment, control activities, information and communication and monitoring—as well as how businesses initiate, record, process and report transactions. The SAS offers auditors some direction by pointing out these key aspects of the systems and controls on which organizations today rely.

SAS no. 94 also looks at the benefits IT provides as well as the risks to an entity's internal control and gives examples of each. The overall picture it presents is that the organizations use IT to achieve their objectives, their use of IT affects internal control and the auditor should expect to encounter IT systems and electronic records rather than paper-based documents.

SAS no. 94 also provides guidance to help auditors determine whether specialized skills are needed to consider the effect of computer processing on the

audit, to understand the controls, or to design and perform audit procedures.

SAS no. 94 clarifies what the auditor needs to know to understand the automated and manual procedures an entity uses to prepare its financial statements and related disclosures. Included are the procedures an entity uses to:

1. Enter transaction totals into the general ledger.
2. Initiate, record and process journal entries in the general ledger, including the procedures for standard entries required on a recurring basis and nonstandard entries to record nonrecurring or unusual transactions and adjustments.
3. Record in the financial statements recurring and nonrecurring adjustments, such as consolidating adjustments, report combinations and reclassifications that are not reflected in formal journal entries.[28]

From the previous, one can see that studies on IS Auditing discussed the contribution of information technology to auditing systems,

[28] For further information visit www.AICPA.com

it's drawbacks, transaction processing and computer control procedures (General Controls and Application

Controls). However, previous studies did not talk about the actual implementation process.

The main goal of this study is to introduce a procedure that can be followed in IS Auditing. The procedure shall be presented in the form of a flowchart which will constitute an IS Auditing Model.

4.4.1 T

Chapter five

Research Methodology

This chapter will concentrate on the basic methodology, our population, how the data was gathered, and the difficulties of the study and the conclusions of the study.

5-1 Research Methodology and Data Gathering:

If we go through the flow charts of the research process, we can recognize that after discovering the problem, the exploratory research technique must be selected. There are four techniques; this study used the Case Study technique, where the case study was conducted on Fastlink Company.

By going further through the flow chart, after determining and defining the problem (statement of research objectives) as stated in chapter one, the research method or design must be chosen. In this study the basic design method will be the survey, the data were gathered through interviews. Each respondent was interviewed in his office; the personal interviews are generally expected to last approximately one hour. A variety of types of research questions were asked, some were open-ended response questions, others were fixed-alternative questions.

A couple of sample questions that were asked are:

- What are the controls implemented to address many of the risks associated with the reliance on IT?
- How often do you evaluate these internal controls?
- In what capacity did computer controls replace manual controls: 1) partially, 2) fully?

Also some fieldwork and observation took place in this research.

5-2 The Statistical Population:

Since the study is a case study on Fastlink Company and was applied on Fastlink, the interviews were conducted with all internal auditors, which are ten auditors, so there was no sample; the study was based on census.

5-3 The Difficulties of the Study:

The subject of the study is a very new one, so there was a difficulty in gathering data about it and obtaining previous studies since it is new, especially that the application of Information Systems Auditing in Jordan is very narrow and only done by foreign CPA companies here in Jordan. Some of the important information for this study is very restricted and cannot be accessed or published for all companies.

5-4 Findings:

After conducting the interviews and gathering information about the auditing process in Fastlink, a model for IS auditing has been concluded. The model has proved that it takes less time and may reduce loss caused by Information Systems implementation.

The steps of this model are not very different from the auditing process in manual systems, but with some changes it proved its effectiveness in the field of IS.

This model could be expressed in the following steps (Audit plan):

Step one: In auditing Information Systems, it is essential to classify the company's operations into cycles, in Fastlink the cycles are classified as follows:

a) Revenue cycle.
b) Expenditure cycle.
c) Fixed assets.
d) Inventories.
e) Payroll and personal.
f) Treasury.
g) Investments.
h) Equity.

Step two: The most important point that has been concluded in this study is the beginning of the audit. The audit must begin with the riskiest cycle of the firm's operations, in order to determine this; each cycle has been divided into processes. To determine that, a risk model has been clarified for this matter for each process in each cycle.

5-4,1 Preliminary risk assessment:

Overview:

A study has been carried out to determine a schedule of priorities for audit attention.

In order to prepare this document, an audit risk model was adopted, predicated on the basis that all risks are relative but combining three key factors can compare them:

1. The size of the risk or exposure.
2. The likelihood that the risk will materialize.
3. The probability of the consequences being detected if the risk does materialize.

Each of these three factors were given an equal overall weighting to reflect the fact that audit assessment is a combination of risk and control.

The risk in each department or division throughout the company was then evaluated to create a score for each of the three categories above. The sub-categories were given different weights to reflect their relative importance.

The overall scores were combined to create an overall risk assessment.

Results of this preliminary risk assessment were presented diagrammatically.

5-4,2 Audit Risk Analysis Model:

The following criteria were assessed and the scores were entered in a PC model to get the final risk assessment.

1. SIZE: *parameters relating to the size of the exposure or risk:*

   A= Value of income or expenditure, or size of budget.

   1: up to $2m

   2: between $3m and $20m.

   3: between $21m and $100m.

   4: between $101m and $200m.

   5: over $200m.

   B= Number of employees involved.

   1: up to 100.

   2: between 101 & 500.

   3: between 501 & 1000.

   4: between 1001 & 2000.

   5: over 2000.

   C= Impact on the Company.

   1: negligible.

   2: small.

3: significant.

4: potentially serious.

5: potentially disastrous.

D= Volume of transactions.

1: fewer than 500 per month.

2: between 500 & 2499 per month.

3: between 2500 & 4999 per month.

4: between 5000 & 14999 per month.

5: 15000 or over per month.

2. CONTROL: *parameters relating to the likelihood of the risk materializing:*

F= Impact of management and staff, this includes many issues such as the quality of management, extent to staff turnover, length of time an operation has been within the business, degree of expressed concern by the management, and the staff's morale.

The score was given a range from "1" to "5" where "1" represents top quality management and staff with low turnover of both, in an operation which has been in existence for more than three years and about which no known concern is being expressed.

G= Third party sensitivity, such as tax implications, extent of regulatory requirements, legal implications, and joint ventures.

The score was given a range from “1” to “5” where “1” means there are no tax legal regulatory or other third party implications and “5” means that very significant third party sensitivity is present.

H= Standard of internal control, this includes issues such as extant to losses, vulnerability to fraud, extent to which standard systems are being used, extent to which operating manuals are complied with, reliability of last internal control review, extent of weaknesses highlighted in last internal control review, and strength of accounting systems.

Standard of internal control was given a range from “1” to “5” as follows:

1: Excellent.

2: Above average.

3: Sound.

4: Known or suspected to be weak.

5: Known or suspected to be very unsound.

J= Inherent operational risk, this includes issues such as inherent risk assessment from last audit, control rating from last audit based on audit findings and recommendations, the extent to which the project or activity is speculative, and the extent to which commercial circumstances are changing.

The score was given a range from “1” to “5”. A score of “5” should be given if the operation’s inherent risk is considered to be very high.

K= Likelihood of occurrence.

1: Rare.

2: Unlikely.

3: Possible.

4: Likely.

5: Almost certain.

3. DETECTION: *parameters relating to the probability of unwanted consequences being detected if they do materialize.*

   L= Likely effectiveness of internal audit, this includes issues such as willingness and ability of clients to react positively to results of audit, extant to which relevant specialist skills are available to internal audit,

ability to conduct a competent audit, the degree of need for thorough audit follow-up, the quality of internal audit systems documentation, knowledge of business and experience of staff, and involvement and availability of management.

The score was given a range from “1” to “5”. A score of “5” should be given if there were no significant constraints that are likely to preclude doing an effective audit, for example, a well-established function with fully experienced and trained staff with good knowledge of the business together with respective and focused line management.

M= Duration of the audit:

1: Over 16 man weeks.

2: 12 – 16 man weeks.

3: 8 – 11 man weeks.

4: 4 – 7 man weeks.

5: Less than 4 man weeks.

N= Length of time since the last audit:

1: Less than 6 months.

2: Between 6 and 12 months.

3: Between 13 and 18 months.

4: Between 19 and 24 months.

5: More than 24 months or never audited.

P= Effectiveness of other assurance providers:

1: Regular internal, quality assurance and other audits with no significant findings.

2: Regular internal, quality assurance and other audits with some significant findings.

3: No other audit work completed.

4: Regular internal, quality assurance and other audits with many significant findings.

5: Continual significant problems identified by assurance reviews.

In order to assess the risk for an operation a formula has been adopted as follows:

SIZE CONTROL DETECTION

$$\frac{(2A + B + 3C + D)}{35} \times \frac{(2F + G + 3H + 2J + 3K)}{55} \times \frac{(L + 2M + 2N + 2P)}{35}$$

The result is multiplied by 200.

Assessment of results:

Score:

>80 Top Priority.

60 – 79 Critical topic for review.

40 – 59 Important to tackle.

20 – 39 Lower priority but still valid audit topic.

<19 Audit probably unnecessary.[29]

Step three: After determining the preliminary risk by using the previous model for each process in each cycle, the third step is to set controls to address each of these risks beginning with the riskiest, because these risks if not well controlled may cause serious losses.

In determining the controls, it was mainly based on personal and professional judgement of the auditor, the nature of the risk and the nature of the company's operations and auditing system.

In many cases some risks already have controls set previously. In such cases the risk is assessed, then the auditor determines the grade for the existing controls. This grade is set based on professional judgement as mentioned above. In these cases, after assessing the risk and the grade for the existing controls the auditor can extract the exposure, which is the difference between the risk and the control grades.

[29] *This formula was given to Fastlink Company from Dilloit (Auditing Co.).*

For example:

By applying the risk equation presented before, the risk Range will take the rating between 1.6 ➔ 200, the controls will be given the same rating between 1.6 ➔ 100. After applying our risk model it appeared that the concerned risk had a grade of 90 (which is considered high). After taking an idea of the controls related to the concerned risk the auditor assessed the controls to take a grade of 25 (which is considered low compared to the risk). So in this case the exposure will be:

90 – 25 = 65.

In these cases the priority is given to the highest exposure not the highest risk.

Step four: After setting the controls for each risk, these controls were applied to address the risks.

Step five: An audit draft report was developed.

Step six: A final audit report was issued in order to get approval from related parties.

Above is the procedure and steps to apply an IS audit. The following is a full example on one of Fastlink's cycles and the results will be presented diagrammatically.

Step one: After classifying the company's operations into cycles as mentioned before it is important to determine the processes in each cycle.
In Fastlink there are eight cycles: Revenue Cycle, Expenditure Cycle, Fixed Assets Cycle, Inventories Cycle, Payroll and Personal Cycle, Treasury Cycle, Investments Cycle and Equity Cycle.

The sales (revenue cycle) will be taken as an example, which has fourteen processes as classified in Fastlink, which are as follows:

1. Ordering and receiving products.
2. Selling products and services.
3. Collections.
4. Scratch cards replacement.
5. Termination and deposit refunds.
6. Customer service.
7. Void transactions.

8.

9. RSS (point of sales) system related controls.

10. Hiring, training, evaluating and termination of retail shop heads and reps.

11. Retail sales commissions.

12. Flow of documents between shops and head office and vice versa.

13. Retail sales planning, forecasting, research and evaluation.

14. Coordination between retail sales and marketing.

15. Retail sale shops security.

Not all risks in each process are related to information systems, but this study will concentrate on risks related to information technology.

In process number eight (RSS-point of sales-system related controls), five risks have been noticed:

Risk 1: Misassigning of privileges to shop reps.

Category ➔ Information Systems.

Description: RSS privileges are not granted properly to shop

reps.

Each risk was evaluated as follows:

a) Consequence (ascending):

- Insignificant.
- Minor.
- Moderate.
- Major.
- Catastrophic.

b) Likelihood (ascending):

- Rare.
- Unlikely.
- Possible.
- Likely.
- Almost certain.

c) Severity (ascending):

- Minimal.
- Low.
- Moderate.
- High.
- Extreme.

As for risk 1, the risk will be major, likely to happen and it's severity will be extreme.

d) Risk: Risks will have a special rating (according to the risk model), so if it took a rating between 1.6➔200 and by using the risk model explained earlier risk 1 will take a grade 90 which is considered high.

e) After assessing the risk, current controls for the same risk will be evaluated based on professional judgment and it will take the same rating between 1.6➔200. For example if the current controls were given a grade 22, the exposure will be 68.

New controls were set, in the case of this risk the new controls were as follows:

- The shop reps should have only the privileges that help them to accomplish their work without having any unneeded privileges.
- Their direct managers should authorize the granting of such privileges.
- MIS follow-up the usage of such privileges.

f) After controls were set for each risk it was essential to apply tests to ensure that the controls were effective in addressing the risk.

For risk 1 the test was:

- Obtain a report from MIS that showed the privileges (commands) assigned to retail sales employees.
- Obtain from retail sales the privileges that should be granted to shop reps.
- Compared the privileges that actually granted with the ones that should be available to them.
- Privileges were granted and removed by specified personal within MIS.

Each risk want throw the same steps.

Risk 2: The privilege of assigning products is granted to ineligible employees.

Category ➔ Information Systems.

Description: The risk of assigning products by

ineligible employees may lead to fraud.

- Consequence: Major.
- Likelihood: Possible.
- Severity: Extreme.
- Risk: 80.
- Control: 30.
- Exposure: 50.

Risk 3: The risk of delay in commands execution regarding customer's features.

Category ➔ Information Systems.

Description: The risk of delay in commands execution regarding customer's features and services which may lead to customer dissatisfaction.

- Consequence: Major.
    - Likelihood: Almost certain.
    - Severity: Extreme.
    - Risk: 160.
    - Control: 0.0
    - Exposure: 160.

Risk 4: Inefficient logical security over RSS.

Category ➔ Information Systems.

Description:

1. Passwords are not changed on a monthly basis minimum.
2. Passwords are not of six digits minimum.
3. Non-existence of a product manual.
4. Non-existence of code documentation.
5. Bach-up for the code and database.
6. Back-up is not being maintained is distinct and protected areas.

- Consequence: Major.
- Likelihood: Likely.
- Severity: Extreme.
- Risk: 120.
- Control: 0.0
- Exposure: 120.

Risk 5: Ineffective physical controls over RSS.

Category ➔ Information Systems.

Description:

1. RSS server is not safeguarded properly (locked and AC).
2. Ineffective access to server room.
3. Non-existence of a back up server.
4. Lack of sensors (fire and water leakage).
5. Consequence: Major.

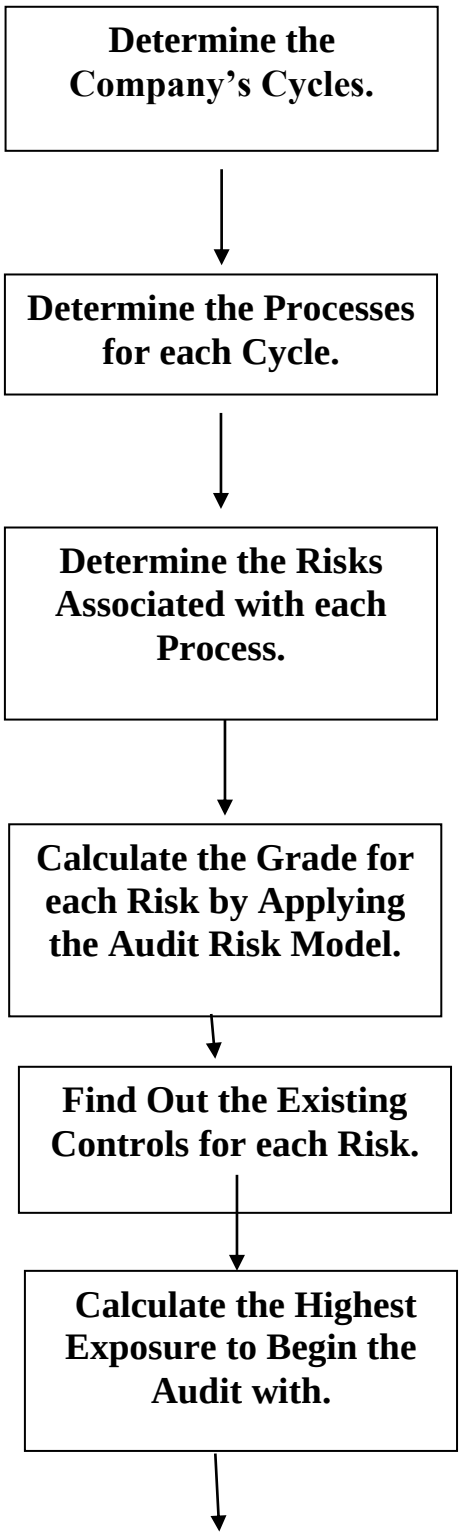
- Likelihood: Likely.
- Severity: Extreme.
- Risk: 120.
- Control: 40.
- Exposure: 80.

After the risks were assessed and the controls were set, a report was issued to clarify the time to begin tests related to each risk. Finally related parties approved the report.

The results were presented diagrammatically and has been attached to this study.

5-5 Conclusions and Recommendations:

By going through the chapter it is obvious that the conclusion of the study is a model to apply an IS audit. This model could be summarized in the following flowchart:



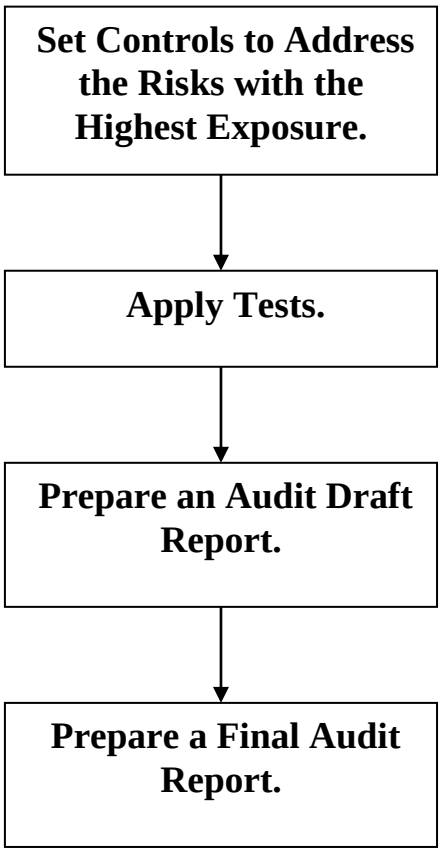


Figure 5-1 IS Audit Model

The most important point that could be recommended in this study is the beginning of the audit. Any IS audit must begin with the riskiest process or cycle of the firm's operations, or the one with the highest exposure, because if these risks occur they may cause catastrophic losses for the firm.

It is also recommended to apply the earlier model, cause it proved it's effectiveness in saving time and cost.

REFERENCES

Arens, A., and, Loebbecke, J., **Auditing: An Integrated Approach**, 8th ed. Upper Saddle River, NJ.: Prentice Hall, 2000.

Arens, A., and Loebbecke, J., **Auditing: An Integrated Approach,** 9th ed. Upper Saddle River, NJ.: Prentice Hall, 2001.

Boynton, W.; Johnson, R.; and Kell, W., **Modern Auditing**, 7th ed. NY.: John Wiley & Sons, Inc. ,2001.

Delaney, P., and Whittington, R., **CPA Examination Auditing**, NY.: Welly, 2002.

Dillard, A.; Jesse, F.; and Beverly, H., **"Technology and Management Control Systems"**, Accounting, Management and Information Technology, Vol. 3, No. 3, 1993.

FASB, Qualitative Characteristics of Accounting, **"Statement of Financial Accounting Concepts No. 2.** Stamford, Conn.: Financial Accounting Standards Board, 1980.

Gupta, K., **Contemporary Auditing**, 5th ed. ND.: Tata McGraw-Hill Publishing Company Limited, 2000.

Hollander, A.; Denna, E.; and Cherrington, J., **Accounting Information Technology and Business Solution**, 2nd ed. NY.: McGraw Hill College, 1999.

Kimmell, D., **Study Guide for Auditing: An Integrated Approach,** 7th ed. Upper Saddle River, NJ.: Prentice Hall, 1997.

Laffie, A., and, Lesli, S., **"E-Filling Security"** Paper Presented at the Tax Division in ProQuset Database, 2001.

Leigh, S., and Others, "Knowledge and infrastructure in international information management: problems of classification and coding", in **Information acumen: The understanding and use of knowledge in modern business"**, edited by Lisa Budfrierman, Routledge, 1994.

Manson, S.; Mccartney, S.; and Sherer, M., **"The use of Information Technology**

in the audit process: illustration from two big audit firms" Paper Presented at the Department of Accounting and Finance and Management, University of Essex, July 1997.

Mayper, A.; Doucet, M.; and Warren, C., "Auditors' Materiality Judgments of Internal Accounting Control Weaknesses", **Auditing: A Journal of Practice and Theory**, Vol. 9, No. 1,Fall 1989.

Nelson, A., and Debra, L., **"Individual Adjustment to Information-Driven Technologies: A Critical Review"** MIS Quarterly, March 1990.

Ojelanki K., and Others, "What does computer support for co-operative work mean: A structuration analysis of computer supported co-operative work." **Accounting, Management and Information Technology,** Vol. 2, No. 1, 1994.

Taylor, D., and Glezen, G., **Auditing: Integrated Concepts and Procedures**, 5th ed. NY.: John Wiley & Sons, Inc., 1991.

Taylor, D., and Glezen, G., **Auditing: An Assertions Approach**, 7th ed. NB.: John Wiley & Sons, 1997.

Tomlin, Roger, “Developing a management culture in which information technology will flourish: how the UK can benefit”, **Journal of Information Technology,** Vol. 6, 1991.

Tucker, George, H., **“IT and the Audit”** The Journal of Accountancy, Academic Search Elite, 2000.

Winters, A.; Alderman, C.; and Guy, D., **Auditing**, 5th ed. NJ.: Thomson Learning, 1999.

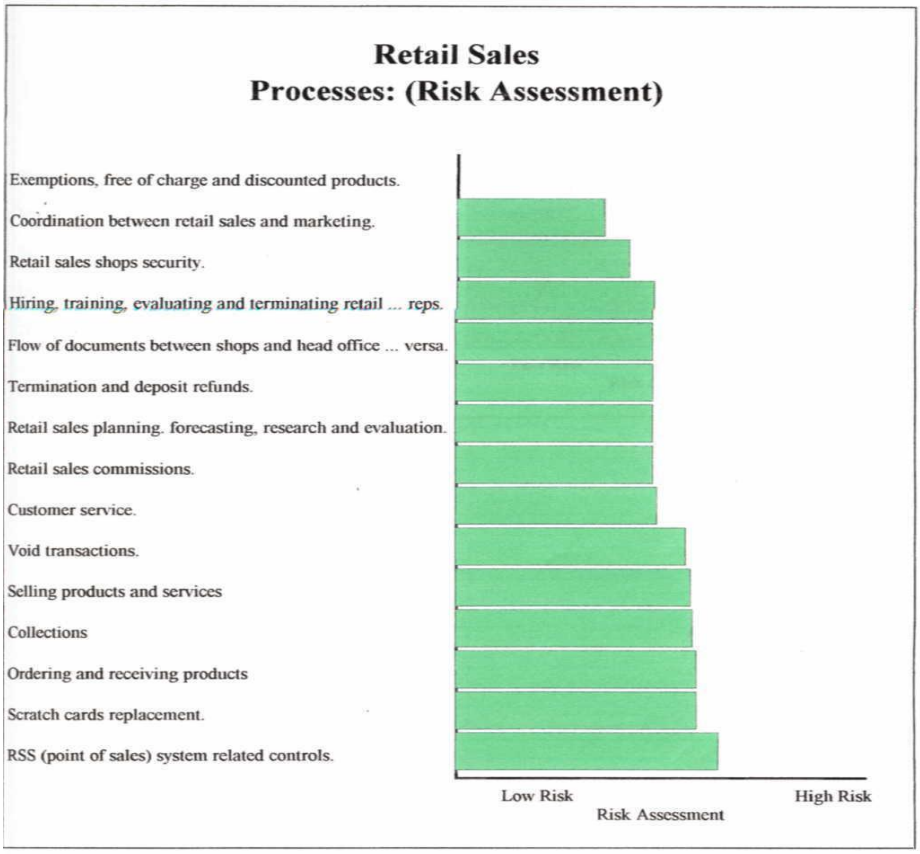
Web Sites:

www.odu.edu.com.

www.ISACA.com.

www.AICPA.com.

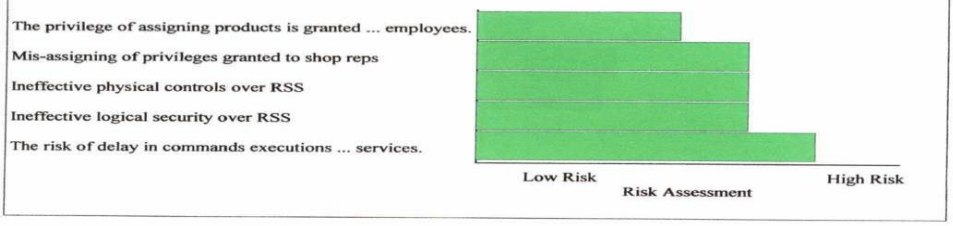
Appendices



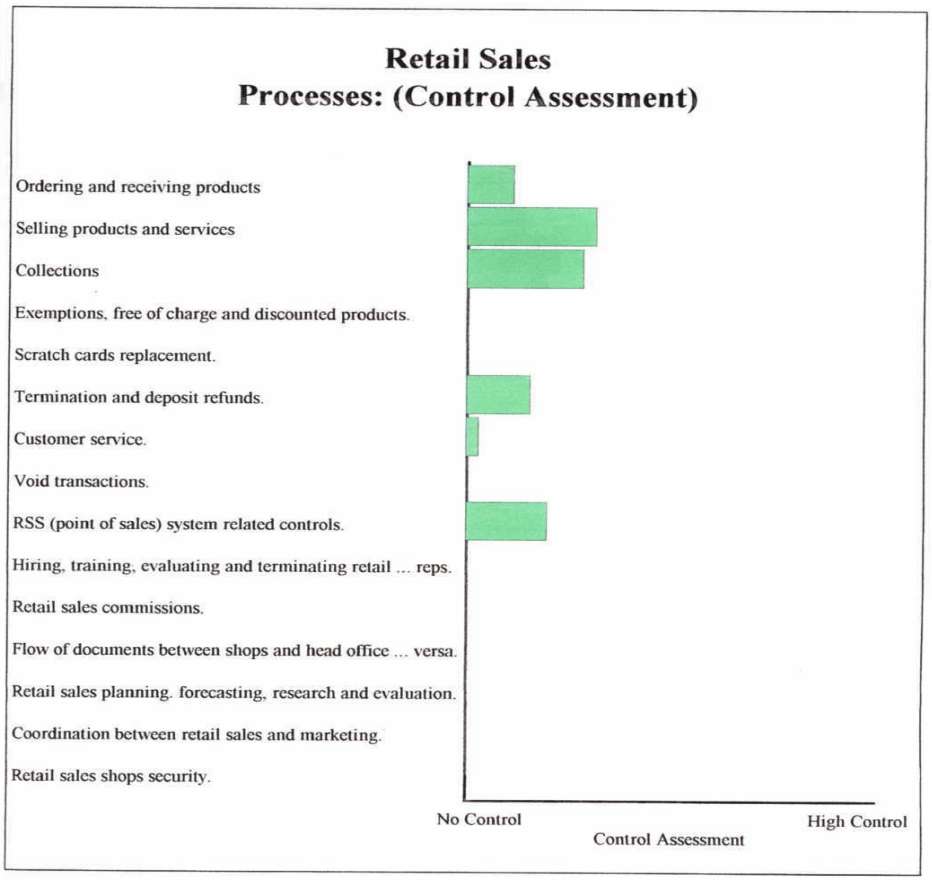
81

Retail Sales

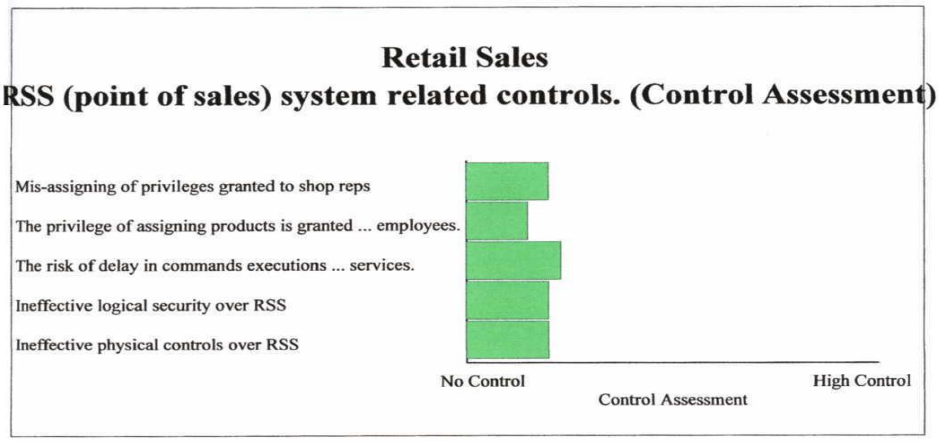
RSS (point of sales) system related controls. (Risk Assessment)



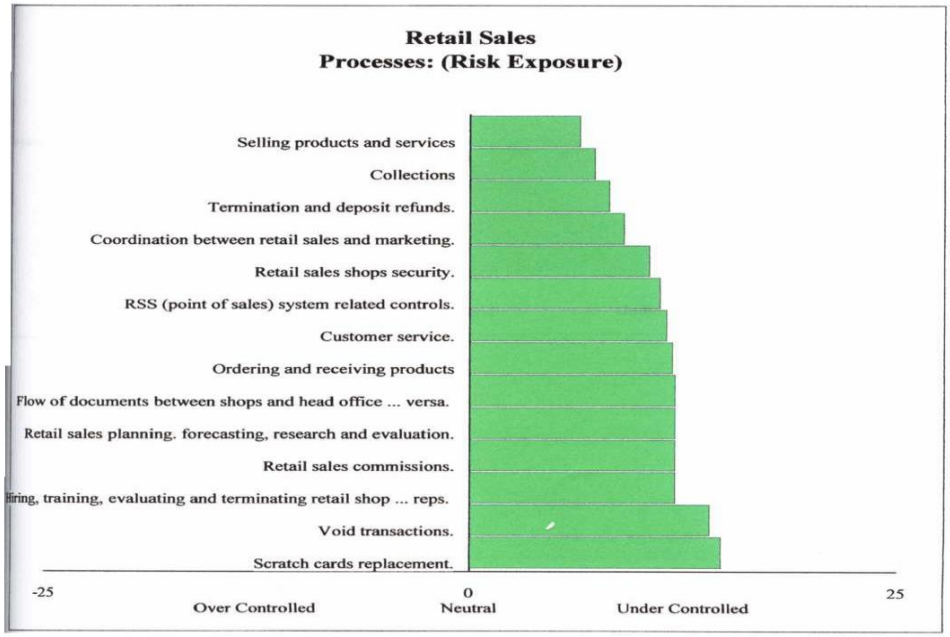
82



83



84



85