INFORMATION SECURITY MANAGEMENT PRACTICES AND ORGANIZATIONAL GOALS: A STUDY OF MICROFINANACE ORGANIZATIONS IN NAIROBI

MADIAVALE BEVERLY AGOSA

D61/72811/2009

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE DEGREEE OF MASTER OF BUSINESS AMINISTRATION (MBA), SCHOOL OF BUSINESS, DEPARTMENT OF MANAGEMENT SCIENCE, UNIVERSITY OF NAIROBI

OCTOBER 2014

DECLARATION

This paper is my own original work. Any assistance I received in its presentation is acknowledged within this paper in accordance with academic practice. I have cited sources for any used data, ideas, words, diagrams, pictures or other information from any source.

Signed___________________________ Date___________________

Beverly Agosa Madiavale

Signed ____________________________ Date__________________

Dr. Njihia

ACKNOWLEDGEMENT

This process has taught me more about research and the world as a whole. I thank God for enabling me through this process. In addition I thank you all including the Microfinance institutions and all the respondents who formed the foundation for this paper.

I acknowledge the assistance from my supervisors Dr. Njihia and Mr. Lelei who played a vital role in shaping this paper by assisting me with knowledge and guidance where necessary.

To my family my greatest thank you for your overwhelming support throughout the whole process.

DEDICATION

This paper is dedicated to my family and the whole student fraternity at the University of Nairobi.

“Special dedication to my dear sons”

TABLE OF CONTENTS

ABSTRACT

The aim of this paper was to study information security management practices and organizational goals in Microfinance organizations in Nairobi. This study looked at whether information security management practices had any relationship or impact on organizational goals. Further, the study sought to identify the various types of information security management frameworks that the organizations had adopted. The specific objectives of the study included establishing types of information security management practices undertaken, extent of awareness of information security management practices by the stakeholders, and how information security management practices are aligned with organizational goals. A census of the population was undertaken of the sixteen microfinance institutions in Nairobi. This was followed by a descriptive analysis of the data collected. The study concluded that most microfinance organizations had adopted information security management frameworks in the simplest form this being ISO. Therefore it was difficult to critically establish the relationship between information security management practices and organizational goals.

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

CISO	Chief Information Officer
COBIT	Controlled Objectives for Information and Related Technology
ICC	International Chamber of Commerce
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management System
ISSM	Information Systems Success Model
ISO	International Organization for Standards
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information technology Service Management
MFIs	Microfinance Institutions
SMEs	Small and Medium Enterprises

CHAPTER ONE: INTRODUCTION

1.1 Background

Information explosion and pressures are leading organizations to investing heavily in IT in order to ensure that IT decisions are aligned to business goals and that risks are managed (Ramani1996). In this regard, information security management (ISM) should be duly considered by organizations whereby ISM describes controls that an organization needs to implement to ensure that it is sensibly managing risks that relate to the protection of information and information infrastructure assets (Risk of loss, disclosure and damages) (Owiti 2011).

According to Norman and Yasin 2010 information security existed even before computer, e.g. encryption has been used since humans knew how to write. IS today encompasses more complex scenario compared to the older days. The introduction of computers together with the developement of the internet technology has changed how we handle and secure information. The evolving of technology and, new business arrangements in distributing information has made it vital for all business owners and business management to consider IT security effort.

Information is today regarded as one of the most valuable assets of an organization and with the advent of globalization and ever changing technologies the need for information security is becoming more and more vital. As organizations are becoming dependent on information technology the emphasis on IS is getting more significant. While initially IS was seen as a technology problem that could be addressed via sophisticated hardware and software solutions, increase in number of security breaches proved that this is indeed mostly a people problem (Rudolph et al 2002). In this regard managing information risks brings together the collective judgments of individuals and groups within these organizations responsible for strategic planning, oversight management, and day-to-day operations –providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of these organizations (NIST, 2011). Thus effective risk management requires that organizations operate in highly complex interconnected environments i.e. systems that organizations depend on to accomplish their missions and to conduct important business-related functions (NIST,2011). It can be argued that since information security is continually evolving, businesses have come to view information as a critical asset, and have increasingly come to depend on public networks to transport sensitive information thus protecting information has become less about technology and more about sustainability of the enterprise itself (ISACA 2009).

1.1.2 Information Security Management Practices

Owiti (2011) defines information security management (ISM) as the controls that an organization needs to implement to ensure that it is sensibly managing risks that relate to protection of information and information infrastructure assets. The emerging trends in information technology (IT) have resulted in organizations using different approaches to effectively manage information security. These approaches include risk-based approach and business aligned security approach.

The growing adoption of information security management practices (ISM) has been driven by the requirement for the information technology (IT) industry to better manage the quality and reliability of IT in business and respond to a growing number of regulatory and contractual regulatory and contractual requirements.

ISM practices include COBIT, ITIL, and ISO/IEC 27000. These practices underpin different areas and requirements within the organization so as to enable it effectively attain its goals both organization and business.

Control Objectives for Information and related Technology (COBIT)'s main focus is on development of clear policies and good practices for security and control in IT. It provides managers with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of IT and developing appropriate IT governance and control in an organization. COBIT ensures ISM and business alignment, ISM enabled business processes, resource optimization and management of risks.

ISO/IEC is a standard for information security industry that includes a comprehensive set of controls and best practices. This standard is intended to serve as a single reference point for identifying a range of controls needed for situations where information systems are used in industry and commerce (Larsen et al, 2006).

Information Technology Infrastructure library (ITIL) focuses on critical business processes and disciplines needed for delivering high quality services. ITIL classifies all business activities under service management and service delivery. This approach defines It quality as the level of alignment between IT services and actual business needs (Larsen et al, 2006).

1.1.3 Information Security Management Practices to Organizational Goals

The complex relationships among missions, mission/business processes, and the information systems supporting those missions/processes require an aligned organization-wide view for managing information security (NIST, 2011). Anttila (2003) further adds that information security in a organization is achieved effectively and efficiently through a systematic ISM that is in line with the company's business objectives. However, often information security practices have been implemented as distinct of business and by information security professionals. Many organizations are currently managing IT security in application 'silos'-lightly target security implementations that are not consistent or integrated across the enterprise. This approach often involves the use of "point security" for specific problems, but does not provide a holistic approach for centralized security management. It may provide short-term benefits to a particular department or business unit, but this is often at the expense of future IT efficiency and effectiveness at the enterprise level (Blaunt, 2007). A solution to such a problem is the approach of aigning all necessary information security actions seamlessly with the business management and business processes and how to take into account the realities and requirements of the modern business environments.

In aligning ISM practices, it is extremely important to manage appropriately the business process of the organization. This is because, in practice (operationally), IS originates from process-related activities and information flows between these activities. Thus, IS is affected directly in real time through process arrangements, tools, and people in practical work (Anttila, 2003). This is possible by integrating various ISM frameworks by strategically being able to map ITIL, COBIT and ISO/IEC 27002 so as to reach an efficient technical and operational level (Knorst 2010). This according to a study done by Eric and Eric (2007), on embedding IS into the organization, can be achieved by addressing the key imperatives of globalization, security investment, culture, and security metrics.

1.1.4 Organizational Management and Business Goals

Businesses have major goals that include increase in profit, larger market share, counter competition and brand identity process. In order to achieve these goals organizations must rely on constant flow of information (Surcel & Amancei 2007). Within this context it is deduced that information has become the lifeblood of modern organizations and is core to most business processes today, therefore necessitating optimal protection. As organizations today deal more with electronic information, they have realized that information security issues need to be accorded great importance in line with other business requirements by focusing on four tactical areas including strategy and business alignment, organization and culture, management and governance, and, technology (Saint- Germain, 2005).

A study done by (CPSTL 2003) reveals that an effective information security strategy is key to meeting business challenges. By treating IS as an enabler of manageable, accountable and scalable access, security becomes the catalyst for safe and open information exchange. From this perspective security is no longer just a straight cost but rather an investment in business growth and development. In addition, information security becomes the vehicle by which new business opportunities are realized and enables business continuity.

1.1.5 Microfinance Institutions in Kenya

The World Bank defines Microfinance Institutions (MFIs) as institutions that engage in relatively small financial transactions using various methodologies to serve low income households, microenterprises, small scale farmers, and others who lack access to traditional banking services (Githinji 2009).

Kenya is an emerging market for micro finance. In 2006, Parliament through the Central Bank of Kenya (CBK) enacted a Microfinance Act that was effected in May 2008. In this regard, the microfinance industry in Kenya has experienced a rapid growth over the years in an attempt to meet the large demand from the estimated 38% of Kenyans lacking access to financial services. This demand for MFIs is high yet the industry is only able to meet about 20% of their demand because of lack of financial resources and the capacity to access risk process and monitor loans (Ambala 2010).

According to the Poverty Reduction Strategy Paper (PRSP) of 1999, a large number of Kenyans drive their livelihood from Small and Medium Enterprises (SMEs). With this in mind, over 100 organizations, including about 50 NGO's practice some form of microfinance business in Kenya. About 20 of the NGO's practice pure microfinance while the rest practice microfinance alongside social welfare activities (Owino 2005). Therefore, development of this sector represents an important means of creating employment, promoting growth and reducing poverty in the long-term (Githinji 2009). As a result of this, the Government of Kenya recognizes that greater access to, and sustainable flow of financial services particularly credit to the low-income households and SMEs is critical to poverty alleviation. Therefore, an appropriate policy, legal and regulatory framework via the Deposit Taking Microfinance Act has been developed so as to promote a reliable and sustainable system of microfinance in the country. In addition, fully fledged microfinance units have been established in the Ministry of Finance (The Treasury) and the CBK.

1.2 Statement of the Problem

The adoption and integration of information communications technology (ICT) into the business process is indeed spreading rapidly and firms seek to improve their efficiency through increased integration of ICT. Information security has too often been viewed in isolation the perception being that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals (ISACA 2009). It is emerging that information security has struggled as a function in most organizations due to changing risk profiles, lack of funding, cultural issues and internal and external threats. In addition ISM problem is characterized by complexity and interdependence.

This point to the need for an aligned approach to ISM, which not only involves technical measures but also policies, procedures and education to ensure that data is treated in an appropriately secure way at all times (Clinch 2009). The reason why the alignment of ISM has often not taken place effectively could be the fact that a company's own leadership system has not yet taken shape to a sufficient degree, resulting in the lack of points to grasp onto. It might also be the case that information security issues are delegated too much and to experts only, who will then create their own position. For example, a study by Makumbi, et al (2012), revealed that some attempts at securing the IT assets though these efforts were largely uncoordinated and that the IT security role was frequently unassigned or allocated to someone without appropriate qualification. Moreover many concepts and basic principles of IS are foreign and difficult to understand for busy business managers (Anttila, 2003). This perception has deep roots in the underlying philosophy that the role of information security is almost exclusively to protect against technology threats and not to help business issues that could stimulate a firm's growth. It is easy for this compartmentalization approach to lead to weakness in security management, possibly resulting in serious exposure both from a financial perspective and operational perspective.

Makumbi, Miriti & Kihonge (2012), on adoption of information security policies by Kenyan SMEs, found that 76.2% of the respondents indicated that they had suffered information breaches within 12 months. These breaches included: inadvertent breaches by users, deliberate attacks, asset theft, equipment failure, backup failure, data theft, site disaster, copyright infringement, and privacy breaches. They also found that a substantial number of SME's including microfinance institutions lacked documented security policies. This lack of adherence to recommended practice could probably explain the high number of reported incidents security policy. It was further noted that they have a weak understanding of information security, security technologies and control measures, and neglect to carryout risk assessment or develop security policies and they also lack the funds, expertise, and time to coordinate and manage security activities. It was also pointed out that SME owners are not supportive of information security in terms of time and budget. With this in mind, Kimwele et al(2010),pointed out that in order to tackle ISM effectively, there needs to be education on IS, creation of more IS awareness programs, and vulnerability seminars need to be held so as to show the gap between proper IS management and the lack of it.

From the above, the study intended to find out the relationship between ISM practices and organizational goals.

1.3 Research Objectives

1. Establish types of information security management practices that microfinance institutions are currently undertaking.
2. Establish to what extent stakeholders are aware of ISM practices within the organization.
3. Determine how well ISM practices undertaken align with organizational goals.
4. Determine to what extent alignment of information security management practices enables organizations achieve their goals.

1.4 Value of the study

This study seeks to better understand how business organizations in Nairobi are able to integrate ISM practices for the attainment of organizational goals.

The study also seeks to gain a greater insight into the various ISM practices that are undertaken by different microfinance institutions with the aim of attaining their strategic goals.

The findings of this research will be useful to various business stakeholders in being able to know the progress being made in their organizations in terms of ISM while making comparison to other businesses. Furthermore, the study will act as reference material to researchers pursuing studies in related fields including lecturers and students.

The government as a stakeholder will acquire greater understanding of functions of the microfinance institutions. The government will thus be able to know where to provide support to so that they can be able to attain their organizational and business goals. As a result of this, they will thus be able to make greater contribution to the national economy.

Professional organizations including ISACA will also be beneficiaries of the study. Through better understanding of how microfinance institutions view ISM practices, this can be a platform for the body to come up with better recommendations on ISM practices that contribute to them being better adopted.

CHAPTER TWO: LITERATURE REVIEW

This chapter will mainly focus on literature that is related to ISM practices and organizational goals.

2.1 Information Security Governance

Information Technology Governance Institute defines information security management governance (ISMG) as the leadership, organizational structure and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives (Larsen, Pedersen & Andersen, 2006). According to Robles et al (2008), the discipline of ISM governance derives from corporate governance and deals primarily with the connection between business focus and ISM related matters of an organization. It highlights the importance of Ism related matters in organizations and states that strategic ISM decisions should be owned by the corporate board, rather than by CIO or IT managers. ISMG has become one of the key focus areas of strategic management due to its importance in the overall protection of the organization's information assets.

A properly implemented information ISMG framework should ideally facilitate the implementation of (directing) and compliance to (control) strategic level management directives. These strategic level directives are usually interpreted, disseminated and implemented by means of a series of ISM related policies (Solms, Thomson & Maninjwa, 2006). ISM goals can only be achieved if the policies and procedures are complex, accurate, available and ultimately executed or put into action (Robles et al, 2008).

2.2 Information Security Management Practices

Information security managers have struggled to create programs that are aligned withenterprise goals and priorities, that bring value to the enterprise, and that support the ability of management to innovate while controlling risks. A number of best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls and comply with governance requirements as well as privacy and information security regulations (Ozbilgin). These include three major practices namely; ISO/IEC, COBIT and ITIL.

2.2.1 ISO/IEC 27000

According to Janshcob & Trinstifa (2006 as cited in Shaikpour et al, 2012), ISO/IEC 27000 specifies requirements for the design and implementation of an appropriate ISMS in the organization ensuring that adequate and appropriate controls are selected to protect information assets and to give confidence to interested parties. This is a specification for ISMS and it sets out 'general requirements' (uses words like "must" and "shall").

It comprises eleven security domains and seeks to address security compliance at all levels. These domains are as follows: Security Policy, Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communication and Operations Management, Access Control, Information systems acquisition, development and maintenance, Information security Incident Management, Business Continuity Management, and, Compliance. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of organizations either public or private

There are four established ISM standards in the ISO/IEC 27000 family including ISM System Requirements (27002:2005), Code of Practice for ISM (27002:2005), Information Security risk Management (27005:2008) and Requirements for Bodies Providing audit and Certification of ISM Systems (27006:2007).

2.2.2 ITIL

Information Technology Infrastructure Library (ITIL) emerged in the 1980's and was first developed by the British Central Computer & Telecommunications Agency. It is a framework of best practice guidance in Information Technology Service management (ITSM). It describes processes, functions and structures that support most areas of IT service management, mostly from the viewpoint of the service operator. ITIL also presents a broad set of management procedures, which apply to all aspects of IT infrastructure, within which an organization can manage its IT operations.

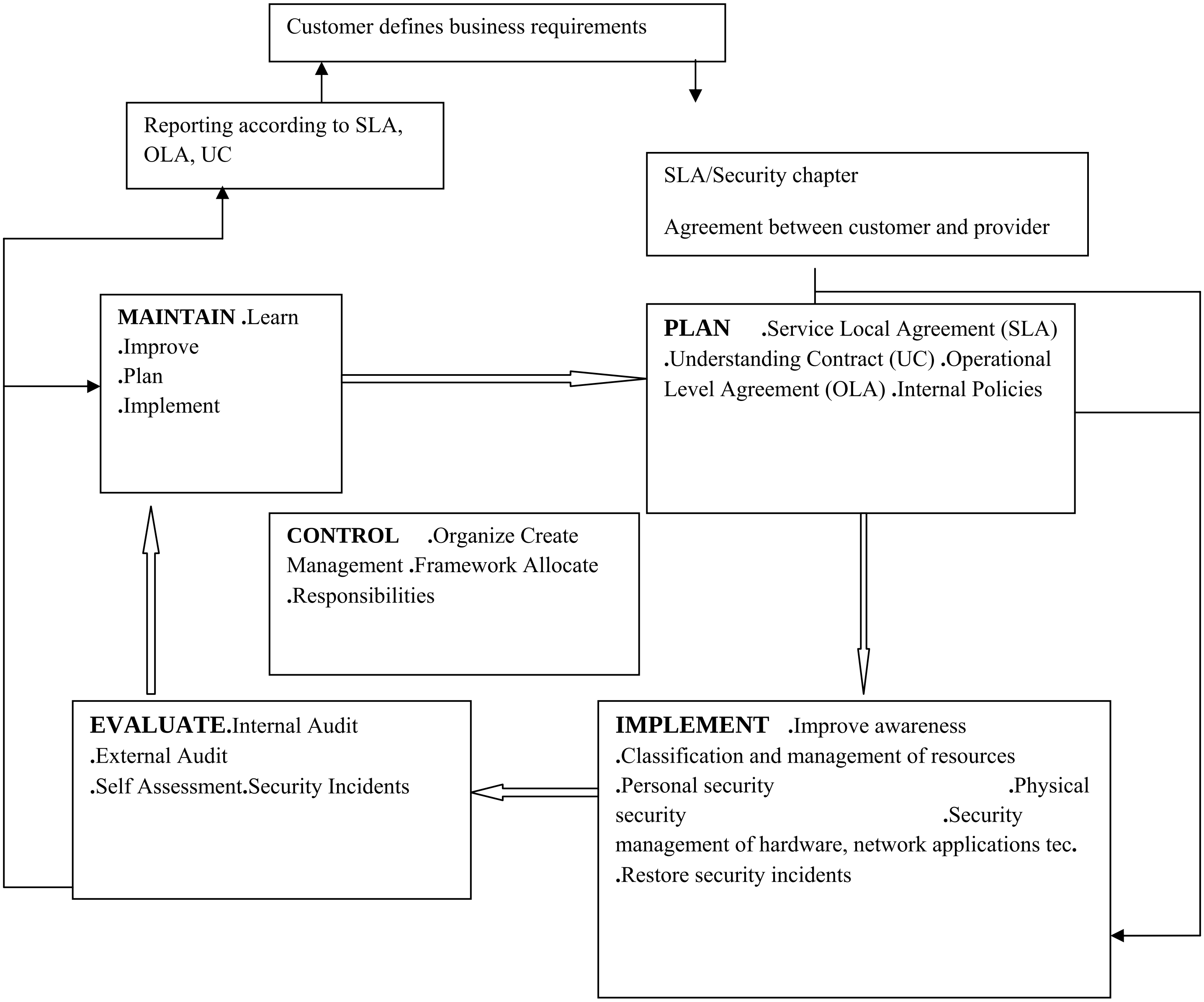
Customer defines business requirements
Reporting according to SLA, OLA, UC
SLA/Security chapter
Agreement between customer and provider
MAINTAIN .Learn .Improve .Plan .Implement
PLAN .Service Local Agreement (SLA) .Understanding Contract (UC) .Operational Level Agreement (OLA) .Internal Policies
CONTROL .Organize Create Management .Framework Allocate .Responsibilities
EVALUATE.Internal Audit .External Audit .Self Assessment.Security Incidents
IMPLEMENT .Improve awareness .Classification and management of resources .Personal security .Physical security .Security management of hardware, network applications tec. .Restore security incidents

Figure 1.ITIL Security Management Framework (COGC 2007)

Gehrmann (2011) further adds that ITIL is a library of good practices related to the service of IT. The best practices are geared towards five areas including service strategies, service projects, transition services, service operation and continuous improvement services. Service strategy provides guidance for the scope, development and implementation of service management based on the capacity and organizational strategy perspectives. Service projects include the guidelines for design and development of services and process related to IT. Transition services, combines practice in the management version, program management and risk management and places them in the context of management service practice. Service operation incorporates the practices of servicing objectives in order to achieve effectiveness and efficiency in the delivery and support services to ensure a value for the customer and the service provider. Continuous improvement services guides the creation and maintenance of values for customers through a better conception, implementation and operations of the services.

2.2.3 COBIT

The Control Objectives for Information and related Technology (COBIT) is a certification created by ISACA and IT Governance Institute (ITGI) in 1996. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues.It entails a set of 34 high level control objectives for each of the IT processes that are grouped into four domains namely: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor.

COBIT has five governance areas of concentration which include strategic alignment, value delivery, resource management, risk management and, performance measurement. Strategic alignment focuses on ensuring the linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing cost, and proving the intrinsic value of IT. Resource management is about the optimal investment and the management of critical IT resources. Risk management is a clear understanding of the enterprises appetite for risk, understanding of compliance requirements, and transparency into the organization. Performance measurement racks and monitors strategy implementation, resource usage, project completion, process performance and service delivery.

2.3 Organizational Goals

Drucker (2010) defines organizational goals as the ends that an organization seeks to achieve by its existence and operation. Drucker identified key areas in which organizations establish result oriented goals including market share, innovation, productivity, profitability, social responsibility, management performance and development, and physical and financial resources.

Makumbi (2012) emphasizes that organizations of all sizes are now significantly reliant upon information and communication technology for the performance of their business activities. Organizations therefore need to ensure that their systems and data are appropriately protected against security threats. Organizations therefore need a single, consistent management system necessitating careful selection of elements and processes from various sources to be integrated into it covering all the areas necessary to support the organization’s business interest (Clinch 2009). Clinch adds that elements including policy, planning, implementation and operation, performance assessments, improvement and management review should be present in recognizable form in any standards or best practice-derived management system and can be regarded as bedrock for building an organizational management system to integrate elements of management system standards.

2.4 Aligning Information Security Management and Organizational Goals

According to ITIG and OGC (2006), the use of standard and best practices is being driven by business requirements for improved performance, value, transparency and increased control on IT activities. As every organization tries to deliver value from IT while managing an increasingly complex range of IT related risks, the effective use of best practices can help to avoid re-inventing the wheel. It also helps to optimize the use of scarce resources and reduce the occurrence of major IT risks such as project failures, wasted investments, security breaches etc.

Best practices that are adopted have to be consistent with the risk management and control framework appropriate for the organization, and integrated with the methods and practices that are being used. Their effectiveness depends on how they have been implemented and kept up to date. In regard to these the various best practices are integrated into the organizational and business goals at different levels and functions of the organization. This is because these best practices are designed to incline towards different organizational functions and at some point they integrate with each other (map onto each other).

COBIT can be used at the highest level of IT governance and it provides overall control since it is a control and management framework rather than a process framework. It focuses on what an enterprise needs to do, not how it needs to do it and the target audience is senior business management, senior IT management and audits. Its main theme is business oriented. It integrates into organizational goals by being able to identify and clarify operational risks that can be detrimental to the business process.

ITIL aligns the IT aspects of the organization with the business aspects in that it is mainly concerned with IT aspects in terms of service support and service delivery. It provides a comprehensive, consistent and coherent set of best practices for IT service management and related process. It provides a quality approach for achieving business effectiveness and efficiency in the use of IS.

2.5 Theories of Information Security Management

2.5.1 Information System Success Model

Information systems success model (DeLone and McLean, 1992) is the most well known for studying information systems success (Wang et al., 2005). The model intimates that information systems quality characteristics (system quality), quality of information systems output (information quality), consumption of information systems output (usage) and user reaction to the information systems (user satisfaction) are important to information systems implementation success.

2.5.2 Business Model for Information Security

Business model for information security (BMIS) was created by Dr. Laree Kiely and Terry Benzel. The model takes a business oriented approach to managing information security. It entails a holistic and dynamic approach to IS within the context of business and demonstrates to the enterprise that IS can be both predictive and proactive.

2.5.3 Comparison of ISSM and BMIS

The ISSM emphasizes that for successful management of IS, the technological systems in place must be very efficient, whereas the business model is independent of any particular technology or technological changes over time and it includes not only traditional IS but also privacy, linkages to risk, physical security and compliance.

In regard to these comparisons it is evident that in both models, there has to be a relationship between the various elements involved. In ISSM the information systems are the underlying aspects and thus they have to relate well whereas in the business model, which is viewed as a pyramid shaped structure, all aspects have to be managed well or the equilibrium is lost.

2.6 Conceptual Framework

This framework tends to give a visual aspect of the study at hand. It enables better understanding between ISM practices and the impact on organizational goals.

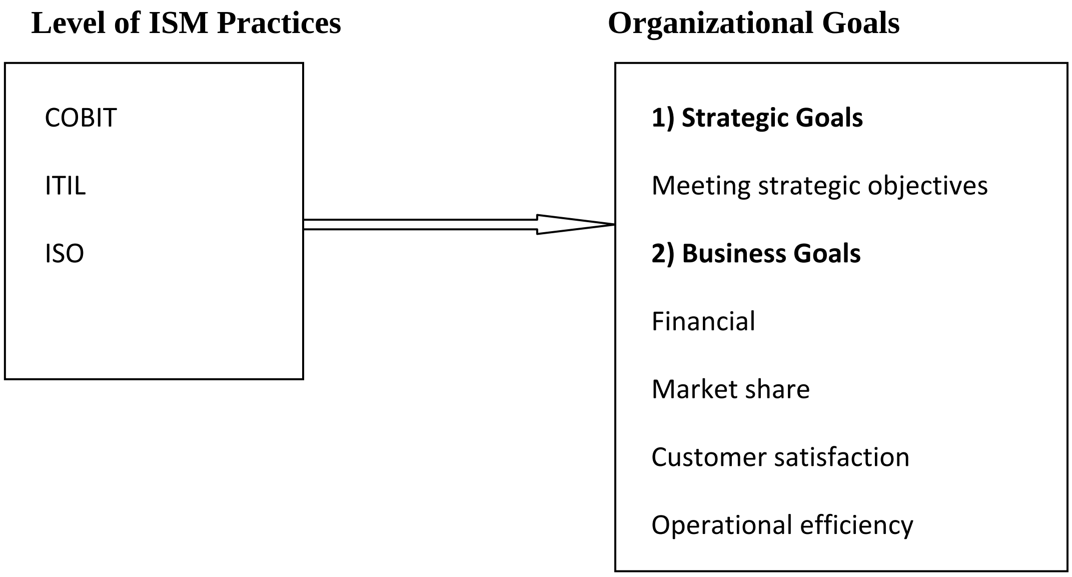

Figure 2. Conceptual Framework for ISM Practices and organizational Goals

2.5 Summary

With information being an important aspect of the organization it is becoming evident that ISM practices are essential to attaining organizational goals. This study proposes to explore to what level microfinance institutions are undertaking these practices and how they are impacting on their organizational goals.

CHAPTER THREE: RESEARCH METHOLOGY

3.0 Introduction

This chapter mainly dealt with how the research was conducted and where it was done. It entails how the relevant data relating to the study was collected and analysed.

3.1 Research Design

Research design is the blue print that enables the investigator to come up with solutions to problems and guides in the various stages of the research.

This study was a descriptive study. This method is advantageous for research due to its flexibility. The data type employed in the study was quantitative

3.2 Population and Sampling

It consisted of all 16 microfinance organizations registered by CBK and operate in Nairobi. Since the study was a census all the 16 MFIs operating in Nairobi were selected for the study. Thus, there was no sampling of the MFIs to come up with a sample size.

3.3 Data Collection

In this study, the main instruments of data collection were questionnaires and interviews. A total of 48 questionnaires were administered with each organization receiving a maximum of 3 questionnaires. The questionnaires consisted of closed and open questions. The questions were divided into three sections. Section A contained general information about the organization, section B focused on ISM practices while section C focused on ISM practices in relation to organizational goals. The target groups for the questionnaires were IT personnel and managers. Completed questionnaires were picked from the various institutions

Interviews were administered in the event that more clarification was required for a particular area.

3.4 Data Analysis

Data analysis was guided by the research objectives designed at the beginning of the research. The data presented in this report was analysed using descriptive analysis and simple linear regression. In descriptive analysis, percentages and frequencies together were computed and measured for each item that measured the relationship between ISM practices and organizational goals. This was followed by simple linear regression analysis to examine the extent to which levels organizational goals are achieved.

The quantitative data collected was coded for ease of tabulation. With the aid of computer software Statistical Package for Social Science (SPSS) statistics were generated.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the study results and interpretation. The study questionnaires were administered to all 16 microfinance organization as per the Central Bank of Kenya list (CBK). Each MFI was receiving three questionnaires each thus a total of 48 questionnaires. After collecting and sorting the questionnaires, 23 questionnaires were not responded to and hence were not included in the final analysis. Thus the final analysis was done with 25 questionnaires.

4.2 Results

The study achieved a response rate of 52.8%. Out of the 48 questionnaires seeking responses, only 25 questionnaires were responded to. The low response rate was attributed to the fact that whereas each of the sixteen microfinance were given three questionnaires to fill, some filled as anticipated while others consolidated the questionnaires into one response and some posted no response at all.

A summary of the results is summarized as follows:

4.2.1 Organization characteristics

Current number of employees

A majority of the respondents had the number of employees between 50-100 employees. This signifies that currently MFI are relatively small in size.

Table 1: Current number of employees

No. of employees	Frequency	Percent
10-20	1	4
20-50	7	28
50-100	18	72
Total	**25**	**100**

Survey Data 2014

Age of organization

A majority (72%) of the organizations polled indicated that they had been in operation for more than three years.

Table 2: Age of organization (Frequencies)

Age of organization	**Frequency**	**Percent**
1-5	2	8
6-10	9	36
10-15	9	36
Above 15 years	5	20
Total	**25**	**100**

Survey Data 2014

4.2.2 Information Security Management Practices

The study sought to establish the type of ISM framework that MFIs had adopted. A majority (52%) indicated that ISO framework was mostly adopted within their organizations. This was followed by 4% who had adopted ITIL, 4% COBIT, while 40% of the respondents indicated that the organization had not adopted any form of ISM framework.

Table 3: Type of ISM Frameworks adopted (Frequencies)

Framework	**Frequency**	**Percent**
COBIT	1	4
ISO	13	52
ITIL	1	4
OTHERS	-	-
NONE	10	40
Total	**25**	**100**

Survey Data 2014

Awareness of ISM practices

From the table below it is evident that in most of the MFIs, there is a high percentage of lack of awareness in terms of ISM practices. The percentages ranging between 44% and 36% though low indicate that there is strong inclination towards not aware.

Table 4: Awareness of adoption of ISM practices

Factors	**Not aware**	**Slightly aware**	**Moderately aware**	**Well aware**	**Very well aware**
	%	%	%	%	%
Resource Management	44	20	20	8	4
Risk Management	36	28	16	0	12
Service Delivery	40	12	12	20	6
Service Management	36	16	12	20	4
Strategic Alignment	36	28	16	8	4
Business Alignment	36	24	16	8	8
ISM Management	36	32	16	0	8
ISM Policy	36	32	16	0	8

Survey Data 2014

Adoption of ISM practices

From the table below, it is a clear indication that majority of the respondents are not aware of adoption of ISM practices within the organization. This is from the fact that a high percentage ranging between 44% and 36% of the respondents are inclined to the fact of not adopted.

Table 5: Adoption of ISM Practices

Factors	**Not adopted**	**Slightly adopted**	**Moderately adopted**	**Well adopted**	**Very well adopted**
	%	%	%	%	%
Resource Management	44	12	20	12	4
Risk Management	36	24	8	4	16
Service Delivery	44	12	16	16	0
Service Management	44	12	16	16	0
Strategic Alignment	40	28	12	8	0
Business Alignment	36	32	4	4	12
ISM Management	36	28	16	8	8
ISM Policy	36	24	16	44	8

Survey Data 2014

4.2.3 Organizational Goals and ISM Practices

In Tables 6 and 7, the results depict the responses on alignment of ISM practices with organizational goals and achievement of organizational goals respectively. The results are shown in terms of means and standard deviation. In Table 6, there was a five likert scale varying from 1(not aligned) to 5(very well aligned) while in Table 7, the five likert scale was varying from 1(no achievement) to 5(very high achievement). The means thus vary 1 to 5 while the standard deviations indicate the variances on each of the responses. With reference to the results, a mean score below 3 point indicates that the factor had no influence while above 3, indicates that the factor had a significance influence.

Table 6: Alignment of ISM practices with organizational goals

Goals	N	Mean	Std. Deviation
Strategic alignment	24	2.54	1.444
Efficiency	24	2.13	1.227
Effectiveness	23	2.09	1.276
Process management	23	1.91	1.041
Resource management	24	2.00	1.063
Financial management (Profit)	24	1.96	1.122
Market share	24	1.86	1.037
Competitive advantage	24	2.83	1.408
Brand identity	24	2.25	1.294
Operational efficiency	24	2.21	1.179

Survey Data 2014

Table 7: Achievement of organizational goals

Goals	N	Mean	Std. Deviation
Strategic alignment	22	2.41	1.403
Efficiency	24	2.29	1.367
Effectiveness	24	2.25	1.327
Process management	23	2.13	1.290
Resource management	24	2.08	1.139
Financial management (Profit)	24	2.08	1.139
Market share	24	2.08	1.100
Competitive advantage	24	2.33	1.308
Brand identity	23	2.26	1.287
Operational efficiency	23	2.22	1.204

Survey Data 2014

Alignment of ISM practices and organizational goal

The simple linear regression produced an inconclusive result and thus it was difficult effectively establish the relationship between ISM practices and organizational goals.

4.3 Discussion

ISM as a whole are controls that an organization puts in place to manage information risks. This coupled with ISM practices are there to enable organizations attain both organizational goals and business goals. This in turn gives advantage to the organization amongst its competitors.

From our findings, it is evident that MFIs have not put much emphasis into the aspect of ISM practices. It is seen that most MFIs have either not adopted any form of ISM practices (40%) or if they have adopted, they have done so gearing towards the most basic form i.e. ISO (52%) and are yet to upgraded it to more comprehensive types of ISM frameworks that tend to encompass most aspects of the organization in relation to ISM practices. Susanto et al (2011) emphasizes that it is important for an organization to adopt a standard or benchmark which regulates governance over information security. This includes adoption of the major frameworks including ISO, ITIL and COBIT.

In terms of awareness of ISM practices, it is evident from the findings that a larger percentage of stakeholders have little awareness of ISM practices. In addition even those that have adopted any ISM framework, there is inadequate in-depth analysis of these practices. This thus creates a gap between understanding ISM practices and adopting them. According to ISACA (2009), organizations need to ensure more awareness of information security management. This can be through organizations establishing information security policies that are supported by standards. With this in mind, the organizations need to develop ISM programs that take into account how the organization and its people, processes and technologies interact, and how organizational governance, human factors and architecture support or hinder the ability of the organization to protect information or manage risk.

From the simple linear regression conducted, it was not possible to determine the relationship between ISM practices and organizational goals. This was based on the fact that the relationship displayed in the scatter plot was not linear as there were quite a number of significant outliers

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1: Introduction

This chapter focuses on the summary, conclusion and recommendations obtained during the study.

5.2: Summary of findings

The research revealed that MFIs are small organizations in relation to size as most had employees between 50-100. In addition most MFIs had been in operation for a relatively short period of time of between 6-15 years.

The study established that most MFIs had adopted the most basic form of ISM practices.

On aspect of awareness of ISM practices, it was revealed that in most of the MFIs, there is minimal awareness of ISM practices amongst the various stakeholders.

In terms of organizational goals and ISM practices, we were able to establish that ISM practices had very minimal impact on organizational goals. This could be attributed to lack of awareness and inadequate adoption of ISM practices.

5.3: Conclusion

Information being a key asset in an organization needs to be adequately protected. Therefore there is need for standards to ensure the best security practices are adopted and an adequate level of security is attained. In addition to this adequate emphasis on ISM practices needs to be enhanced by MFIs. MFIs need to adopt other forms of ISM practices at a broader level and not just standards. In addition more awareness as pertaining to ISM practices need to be emphasized in the organization amongst the various stake holders. This is because information is central to an organization and thus all stakeholders need to be involved.

5.4: Recommendations of study

The study recommends that MFIs in Nairobi and Kenya as a whole need to put more emphasis on ISM practices while at the same time encompassing IT management.

There is need for MFIs to offer sufficient and effective training to the various stakeholders on aspects pertaining to ISM and ISM practices. This will help equip the stakeholders with more knowledge and better understanding of ISM practices.

In terms of resource management, more need to be allocated towards development and sustainability of ISM practices. MFIs need to stop viewing ISM as a lesser function within the organization but should ensure that it is viewed as a key aspect of organizational management and business development.

5.5 Limitations of the Study

This study was not without limitations. Since the sample population consisted of MFIs in Nairobi, this study did not provide a generalization of MFIs as a whole. In addition, the sample size itself was relatively small which contributed to the low response rate. With an increased sample size, a more detailed analysis of the relationship would have been attained.

Lack of awareness as pertaining to information security management amongst the stakeholders in the MFIs was also a limiting factor. This was compounded by the fact that most of the stakeholders do not have enough knowledge concerning ISM practices.

5.6 Suggestions for further study

There is need to carry out further research on ISM practices and organizational goals. More emphasis should be placed on determining the factors that are inhibiting MFIs from effectively adopting various forms of ISM practices.

REFERENCES

Ambala K. (2010). "*Impact of microfinance performance on SMEs in Kisumu Central Business District: a Study of Kisumu Lake Market Business"*. Maseno University

Anir A.N & Yasin M.N.(2010)."An Analysis of information System security management: The Hierarchical Organizations vs. Emergent Organizations". *International Journal of Digital Society* (IJDS), Vol1

Antitla, J. *Business integrated information security management*

Blount, S.,(2007). *"IT security as a business enabler"*. White Paper.

Clinch, J.,(2009). *ITILV3 and information security.* White Paper.

Delone, W.H. & Mclean, E.R. (1992). Information system success: the quest for the dependent variable. *Information System Research 3 (1), 61-95.*

Drucker P.K. (2002). "Managing in the next society". New York: St. Martins Press.

Gerhmann, M.(). *"Combining ITIL, COBIT and ISO?IEC 27002 for structuring comprehensive information technology for management in organizations*". ISSN 2237-4558.

Githinji, B, W. (2009). "*Factors influencing sustainability of microfinance institutions in Kenya.University of Nairobi".*

Grembergeu, W., De Haes S. & Moons J.(2005). "Linking business goals to IT goals and COBIT process". *Information systems Audit and Control Association.*

ISACA (2008). *"Defining information security management position requirements: Guidance for executives and managers".*

ISACA (2009). *"An introduction to the business model for information security"*

ITIG & OGC (2006). *"Aligning COBIT, ITIL and ISO 17799 for business benefit: management survey".*

Kazem,i M. Khajonei H. & Nasrabadi H. (2012).”Evaluation of information security management system success factors: Case study of municipal organizations”.*African Journal of Business Management* Vol.6 pp. 4982-4989, April 2012. ISSN 82233

Kimwele, M., Mwangi W. & Kimani S. (2010). “Adoption of information technology security policies:Case Study of Kenyan Small and Medium Enterprises (SMEs)”.*Journal of Theoretical and Applied Information Technology*(JATIT).

Kimwele, M., Mwangi W. & Kimani S. (2011). “Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs)”.*InternationalJournal of Computer Science and Security* (IJCSS) Vol. 5

Knorst, A.M. (2010). “Strategic alignment between business goals and information security in the information technology governance content: A study in the automation industry”. Thesis. Unisinos Sao Leopoldo.

Ko, M. & Dorantes C. (2006). “The impact of information security breaches on financial performance of the breached firms: An empirical investigation”.*Journal of Information Technology Management*. ISSN 1042-1319.

Komminemi, K.K. & BabuY.A (2013). “An approach for the assessment of the information security and its measures”.*International Journal of Soft Computingand Engineering* (IJESCE).Vol3 ISSN 2231-2307.

Koskosas, J.V & Asimopoules. N (2011*).* “Information system security goals”.*International Journal of Advanced Science and Technology*. Vol. 27

Larsen, .H.M, Pedersen .K. M & Andersen K. V. (2006). “IT governance *reviewing 17 IT governance tools and analysing The Case of Novozymes A/S”* .Proceedings of the 39th Hawaii International Conference on Systems Science.

Makumbi, .L, Miriti K.E & Kahonge M.A (2012).“An analysis of information technology (IT) security practices: A case study of Kenyan small and medium enterprises(SMEs) in the financial sector". *International Journal of Computer Applications* (IJCA).Vol.57 No. 18.

Ma, Q. Johnston A.C & Pearson M. (2008). "Information security management practices: A Parsimonius Framework". *Information Management and Computer Security* Vol.16 No. 3, 2008 pp 251-270.

Moracli H. & Bahreininejad A.(2013). "Toward a comprehensive framework for evaluating the core integration features of enterprise integration middleware technologies".*Journal of Systems Integration*.

NIST (2011). *Managing Information Security Risk:Organization, Mission and Information System View.*

Ogalo, O.J. (2012). "The impact of information system security policies and controls on firms operation enhancement for Kenyan SMEs".*Prime Journal of Business Administration and Management* (BAM).Vol. 2 pp.573-581.

Owiti, .J (2011). "*Information security management present and future*". ICPAK 27th Annual Seminar.

Ozbilgin, G.I. (2009). *Information security management system*: a Case Study in Turkey.

Rene, S. (2005) "Information security management best practices based on ISO/IEC17799". *Information Management Journal.*

Robles, J.R., Park J. & Kim T.(2008). "Information security control centralization and IT governance for enterprises". *International Journal of Multimedia and Ubiquitons Engennering* Vol.3 No. 3

Solms, R., Thomsom K. & Maninjwa M.P. (2006). *"Information security governance control through comprehensive policy architectures".*

Somaini, J. & Hazleton A. (2008). *Information security management programs: organizational assessment-lessons learned and best practices revealed: Part II*

Susanto, H., Nabil M. & Tuan Y.C. (2011).“Information security management system standards: A comparative study of the big Five”.*International Journal ofElectrical and Computer Science* (IJECS-IJENS) Vol. 11 No.05.

Tawileh, A., Hilto J. & McIntosh S. (2003). *Managing information security in small and medium enterprises: A holistic approach*. Scholl of Computer Science Cardiff University

Tiway, K.D. (2011). “Security and ethical issues in IT: An organizations perspective”.*International Journal of Enterprise Computing and Business Systems*. Vol. 1 ISSN 2

APPENDICIES

APPENDIX 1: QUESTIONNAIRE

Section A: General Information

1)Name of organization: ………………………………(Optional)

2) Current number of employees

□ 10-20

□ 20-50

□ 50-100

3) How long has the business been in operation?.....................................

Section B: Information Security Management Practices (ISM)

4) What type of ISM framaworks has the organization adopted? Please tick(√)

□ COBIT

□ ISO

□ ITIL

□ OTHERS

□ NONE

5a) What areas are the stakeholders aware that ISM practices have been adopted

Scale:1=Not aware 2= Slightly aware, 3= Moderately aware, 4= Well aware, 5= Very well aware

5b) What levels of ISM adoption are the stakeholders aware of?

Scale:1=Not adopted 2= Slightly adopted, 3= Moderately adopted, 4= Well adopted, 5= Very well adopted

Levels of awareness **Levels of adoption**

	1	2	3	4	5		1	2	3	4	5
Areas of ISM Practices											
Resource management											
Risk management											
Service delivery											
Service management											
Strategic alignment											
Business alignment											
ISM policy											

Section C: Organizational Goals and ISM Practices

6a) How well are ISM practices aligned with organizational goals?

Scale:1=Not aligned 2= Slightly aligned, 3= Moderately aligned, 4= Well aligned, 5= Very well aligned

Levels of alignment

	1	2	3	4	5
Goals					
Strategic alignment					
Efficiency					
Effectiveness					
Process management					
Resource management					
Financial management(Profit)					
Market share					
Competitive advantage					
Brand identity					
Operational efficiency					

7) To what extent does your organization achieve the following goals?

Scale:1=No achievement 2= Low achievement, 3= Moderate achievement, 4= High achievement, 5= Very high achievement

Levels of achievement

	1	**2**	**3**	**4**	**5**
Goals					
Strategic alignment					
Efficiency					
Effectiveness					
Process management					
Resource management					
Financial management(Profit)					
Market share					
Competitive advantage					
Brand identity					
Operational efficiency					

APPENDIX 2: List of Microfinance Institutions in Nairobi

Faulu Kenya Ltd

SMEP DTM

Uwezo DTM

Kenya Women Finance Trust Ltd

SUMAC DTM Ltd

U&IDTM Ltd

Rafiki DTM Ltd

Remu DTM Ltd

Century DTM Ltd

Aga Khan Foundation (First Microfinance Agency)

Kenya Akiba Microfinance Ltd

Finikiwa Microfinance Ltd

Eurocrest Microfinance Company Ltd

Century DTM Ltd

Mega Microfinance Ltd

Nationwide Microfinance Ltd