A Proposed Information Technology Audit Framework For Microfinance Kumasi

Dr. Thomas Yeboah

ABSTRACT

Information Technology Audit (ITA) has become very important aspect in the Information Technology (IT) industries today since it helps to minimize some of the irregularities in institutions/industries. The Defense-in-Depth (DiD) theory has been accepted by most information security specialists and has been adopted by the Department of Defense (DOD) as a general methodology for improving any organization's information security posture. It means therefore that every IT Audit framework developed should gear towards the Defense-In-Depth theory. It has been observed from documentary pertaining information Technology Audit that none of today's information technology (IT) audit frameworks incorporate all aspects of the DiD theory.

In this research work the researcher identified shortcomings of some accredited existing IT audit frameworks, in particular, relating to Micro finance institutions and develop IT audit framework that addresses the main aspect of Defense-in-Depth (DiD) theory. Therefore, the main purpose of this research work is to come out with a holistic Information Technology Audit framework that incorporates the general aspects of Defense-in-Depth (DiD) theory that can serve as a guide in Information Technology Audit for micro finance institutions in Ghana.

Keywords: *COBIT, Information Technology Audit, COSO ERM, ISO, Defense-In-Depth (DiD), Department of Defense*

Introduction

The Defense-in-Depth (DiD) is considered by most Information Security experts as a best practice for information security, and has been incorporated into different information security fields, such as network protection (Kelly, 2006). This means that in developing an IT audit framework one should keep in mind the Defense-in-Depth (DiD) theory since it forms the basis of the IT audit framework. This research seeks to review most of the accredited IT Audit frameworks and identify some of the shortcomings pertaining these IT Audit frameworks. The Accredited IT Audit frameworks such as Control Objectives for Information and related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management-Integrated Framework (COSO ERM) and International Organization for Standardization (ISO 27001) would be used to form the basis of this research work.

Furthermore, to develop such a framework that will serve as a general guide in Information Technology Audit for Micro finance Institutions in Ghana two research steps have been developed:

a) Identify some shortcomings in these IT Audit frameworks especially those relating to financial institutions (Micro finance Institutions).

b) Develop a holistic IT Audit framework that incorporates the Defense-In-Depth (DiD) theory.

Literature Review

Defense-In-Depth

Defense in Depth is practical strategy for achieving Information Assurance in today's highly networked environments. In every organization Information system forms one of the most significant components of the organization and therefore proper audit should be taken to ensure high security in the organization. The main purpose of information systems auditing is to review and provide feedback, assurances, and suggestions to the organization regarding its information security posture. The National Security Agency (NSA) published the DiD framework that outlines the best practices for information assurance. An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: People, Technology and Operations. as can be seen in Figure 1 that IT Audit framework is based upon.

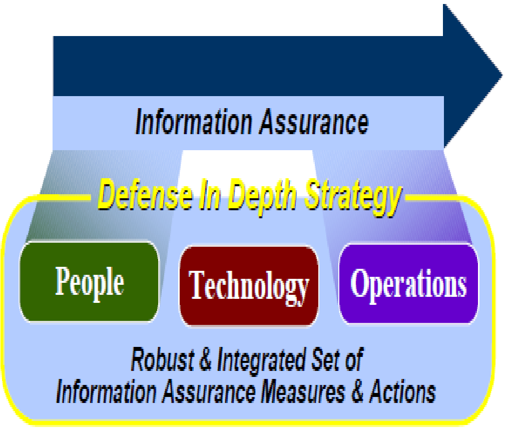

Information Assurance
Defense In Depth Strategy
People
Technology
Operations
Robust & Integrated Set of
Information Assurance Measures & Actions

Figure 1: Defense-In-Depth

In Defense-In-Depth (DiD) theory Achieving Information Assurance begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat. It means that Chief Information Officer (CIO) of the organization should get clear understanding of organization information security. CIO should understands clearly the information being protected and against what threats. This knowledge must be clearly communicated in information security policies and procedures, as well as assignments of roles and responsibilities. This includes training of personnel (National Security Agency, n.d.). Figure 2 gives the people aspect of the DiD theory.

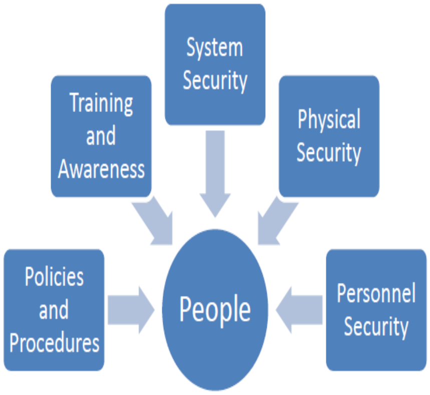


Figure 2: Defense-In-Depth (People)

The second aspect of Defense-In-Depth (DiD) to consider is technology. In today's society there is vast technological advancement for the detection of intruders in organizations. Due to this abundance of technology in providing information assurance for detecting intruders it has become imperative that organizations should have right methods in selecting and implementing these technologies. This can be done through policies and processes such as configuration (National Security Agency, n.d.). Figure 3 gives the technology aspect of the DiD theory.

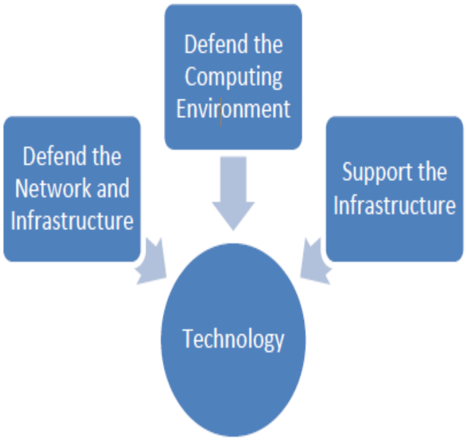

Defend the Computing Environment
Defend the Network and Infrastructure
Support the Infrastructure
Technology

Figure 3: Defense-In-Depth (Technology)

The final aspect of Defense-In-Depth (DiD) theory is operation. This mainly concerns with daily information security assurance in the organization and implementation of policies to remedy future occurrences. Emergency preparedness testing is one of the things an organization has to do to ensure readiness (National Security Agency, n.d.). Figure 4 gives the Operation aspect of the DiD theory.

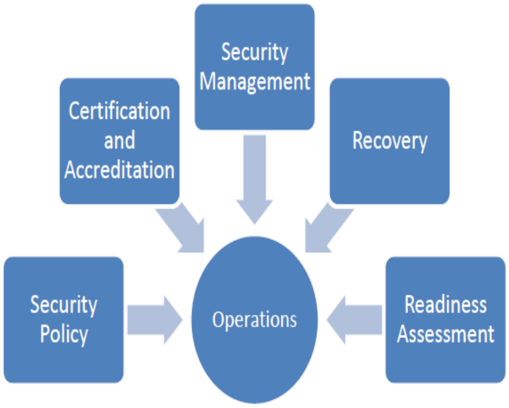


Figure 4: Defense-In-Depth (Operations)

Current Frameworks

In every institutions IT audit must conforms to specific standards or guidelines that needs to be considered for successful IT audit likewise financial institutions IT Audit. The financial sector has very specific regulatory guidelines for conducting an information technology audit (Beaumier, 2007). In today's society some of the accredited IT audit frameworks on the market include the COSO ERM framework, COBIT, and ISO 27002 Code of Practice.

COSO ERM is an organizational framework created by the Committee of Sponsoring Organizations of the Treadway Commission. COSO framework is created to lay out methods for evaluating internal controls for organizations. This organizational framework is created to achieve an entity's objectives, set forth in three categories:

a) Efficient and effective operations
b) Accurate financial reporting
c) Compliance with applicable laws and regulations

COSO report also spelt out five essential components of an effective internal control system:

a) **Control Environment –** This component gives the basic principles on how the organization does their things. The control environment includes the organization's code of ethics, as well as the Board of Directors' oversight and actions and how they affect the integrity and ethical values of the company, including its code of conduct, involvement of the Board of Directors.

b) **Risk Assessment**- The risk assessment component is consider to be the process by which the management use in identifying threats in the organization and how these threats can be eradicated in the organization.

c) **Control Activities** - are generally considered as separation of duties in processing of information in the organization. It mainly internal controls that separate duties within the organizational setup.

d) **Information and Communication** – It is generally deals with how information are communicated both internally and externally by the organization. This usually also includes an evaluation of the organization's technology environment, such as a vulnerability assessment and penetration test.

e) **Monitoring** - is essentially the auditing aspect of the COSO framework and includes a quality assessment of the organization's internal controls, as well as assurance that the organization continues to address new and upcoming risks associated to the organization. (Applegate & Willis, 1999).

COBIT is simply means Control Objective for Information and Related Technology. It is an organizational framework consisting of controls and standards published by the Information Systems Audit and Control Association (ISACA). It is intended as an IT Governance framework that establishes what an organization should do as it relates to IT governance (Meycor COBIT, n.d). Experts claim that one of the main reasons COBIT has been adopted by so many organizations internationally is that it deals with every aspect of IT (Financial Services Technology, 2009). COBIT framework addresses the following area in organizational management and control:

a) **Control Objectives-** This spelt out the control objectives within the organization.
b) **Control Practice-** This area contains explanations of why a certain control objective should be in place.
c) **Auditing Guidelines**- This area of the framework gives how the auditor can gain understanding of the controls as well as measure compliance and develop the residual risk if controls are not adequately implemented.
d) **Management Guidelines** - These provide guidance on how to assess and improve IT process performance.

Therefore the COBIT framework can be summarized in as the one in figure 5

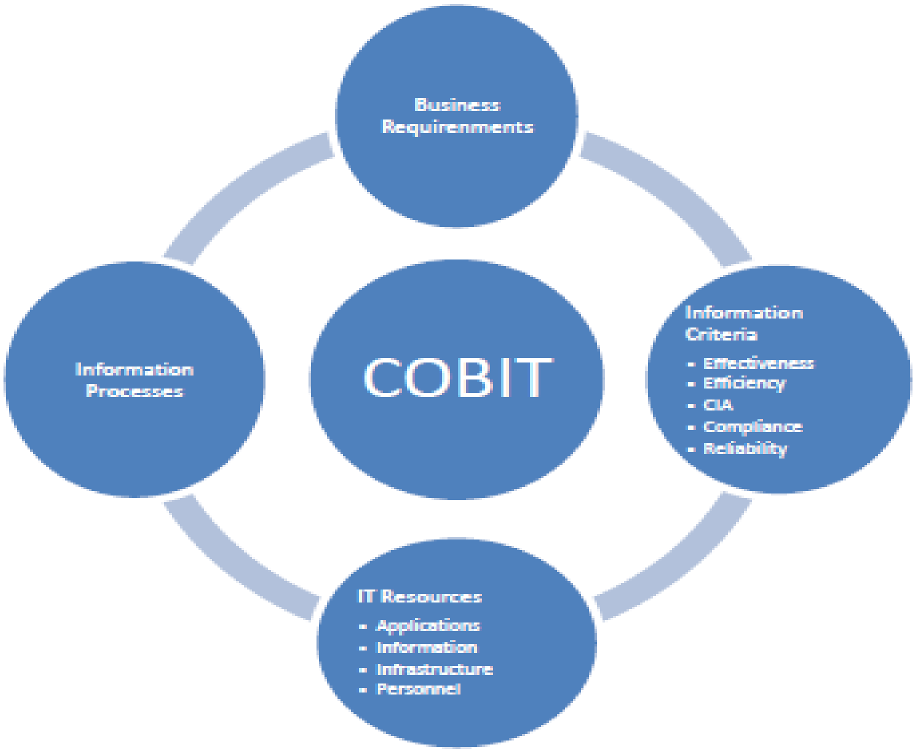


Figure 5: COBIT Framework

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled *Information technology - Security techniques - Code of practice for information security management*.
The ISO guidelines are considered to be an international standard for ―best practices‖ for Information Security, and are the minimum baseline for controls that all information security programs should address in some way, depending on the size and complexity of the organization (Carlson, 2008).
According to (Zhu 2007) the purpose of an ISO 27002 Audit is to check compliance as it relates to the following criteria:

a) The organization’s Security Policies and Procedures
b) Customer and Contract Requirements
c) Legal Requirements (regulatory requirements etc.)
d) The documented Information Security Management System
e) Organizational standards

Methodology

This research study was carried out in order to find out the Information Technology Audit frameworks being used by Micro Finance Institutions in Kumasi and the possible shortcomings of these frameworks.

Sample Techniques

In this study the sampling techniques used was Stratified Sampling techniques. This method is used when the parent population or sampling frame is made up of sub-sets of known size. These sub-sets make up different proportions of the total, and therefore sampling should be stratified to ensure that results are proportional and representative of the whole. The reason why this sampling technique was appropriate for this study is to get the microfinance in Kumasi metropolis that has been existence for the last two years.

Population

The population consisted of some of the microfinance institution in existence for the last two years. The reason for including only these institutions was to delimit the study and minimize certain differences that could emerge due to inexperience of some of the IT auditors.

Data for the study have been collected through a face-to face interview with some IT auditors in various selected microfinance in Kumasi. A sample size of 10 microfinance has been used in the study.

Table 1-1: List of Microfinance Institutions

S/N	Microfinance
1	Bond Financial Services
2	Delex Financial Services
3	Money Link Microfinance
4	TF Microfinance
5	Mpress Microfinance
6	Africa Trust
7	Sinapi Aba Trust
8	Hegis Microfinance
9	Opportunity Saving and Loans
10	Eden Microfinance

Results

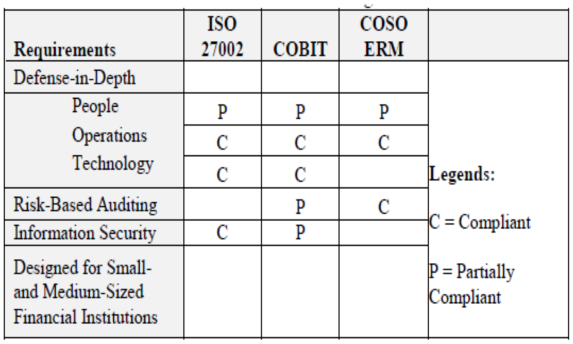
During the analysis stage the researcher tried to compare the various shortcomings of the existing frameworks against the Defense- in- Depth theory to see whether each framework conforms to this theory. The following were the shortcomings identified in these individual frameworks:

COBIT framework - The major drawback identified in COBIT framework is that it is not an Information Security standard. It can be seen clearly in COBIT framework that it has 34 processes, and only one of them relates to information security. Therefore, it may be a good idea to team COBIT with an Information Security standard, such as ISO 27002 (Briggs, 2007). This means that a framework which has both COBIT and ISO 27002 features can be an added advantage to both COBIT and ISO 27002 frameworks. However, COBIT 34 processes as being identified itself is too complex and therefore combining with ISO 27002 framework will make it more complex which can make microfinance IT Auditors find it laborious and boring in using such a framework.

COSO Framework - One of the major problems identified by IT auditors in the various Microfinance used for the study with COSO framework is the fact it provides little or no guidance on how to implement the controls. It was observed from the respondent that to get better results for COSO framework is by combining with COBIT. In doing so also raises another issue increase in the cost of implementation of audit process which can be a problem for some of the microfinance institutions.

ISO 27002 – This framework talks much detail about holistic and managerial approach to IT but fails to talks much about how to conduct an audit if management conveys these important policies and procedures to employees of the organization. A summary of the results is outlined in table 1-2. If an item is marked with a 'C' it means the component of the framework conforms to Defense- in- Depth theory, item marked with a 'P' is partial fulfillment of the Defense-in- Depth theory and finally if item is not marked it means it does not conform to Defense-in- Depth theory.

Table 1-2: List of Frameworks and Shortcomings



Requirements	ISO 27002	COBIT	COSO ERM
Defense-in-Depth			
People	P	P	P
Operations	C	C	C
Technology	C	C	
Risk-Based Auditing		P	C
Information Security	C	P	
Designed for Small- and Medium-Sized Financial Institutions			

Legends:
C = Compliant
P = Partially Compliant

Proposed Framework

Upon thoroughly consideration of all the drawbacks identified in all the three frameworks being considered the researcher came out with the following framework that can be used by IT auditors in microfinance institutions or every small scale financial institutions. Figure 6 gives the proposed framework for microfinance institutions.

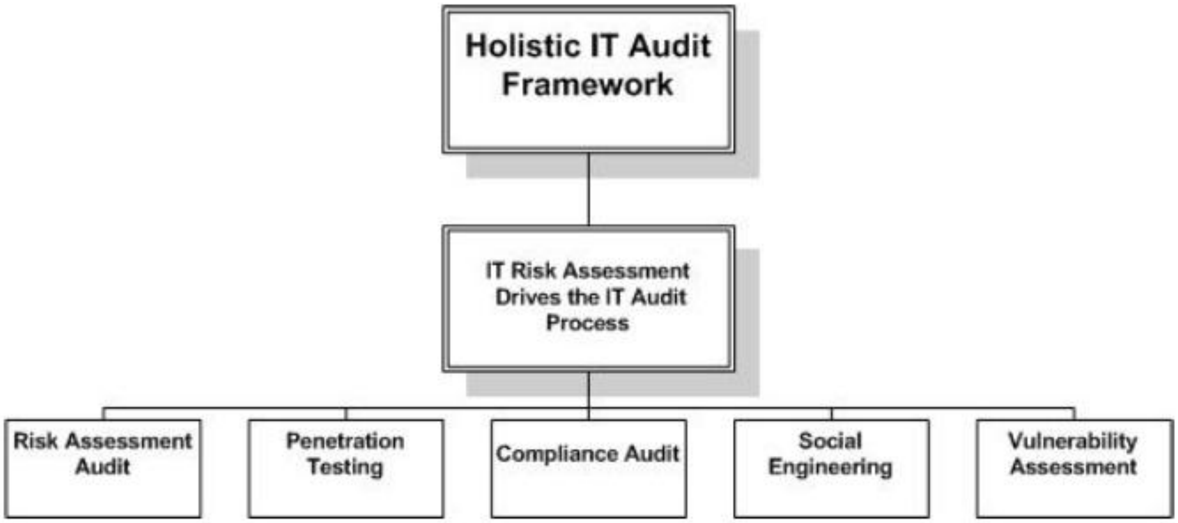


Figure 6: IT Audit Framework for Microfinance

IT Risk Assessment - The risk assessment is an ongoing process of evaluating threats and vulnerabilities and applying mitigation strategies to each asset.
Compliance Audit -The main focus of compliance Audit in this context is a verification of what the organization has in place, and how well it is in place.

Social Engineering -The purpose of the Social Engineering Assessment is to protect the institution's information by identifying weaknesses through the testing of employees and business processes against common social engineering attacks.

Vulnerability Assessment - Vulnerability Assessment tool, also called security scanning tool, is used for an assessment of a particular network or a host system. It scans everything on a network, such as servers, firewalls, routers, and applications for vulnerabilities, and detects known flaws and bugs in software and hardware.

Penetration Testing - Penetration Testing (PT) is another important aspect of a comprehensive IT Audit. It is an analysis of a bank's external network connections (Internet, Feline, Internet Banking, etc.), usually conducted by experts and designed to measure if connections and ports are vulnerable to a series of attacks.

Conclusion

The study was carried out to identify some of the major drawbacks in IT Audit frameworks currently on the market and propose a newly framework that can be used in IT audit for microfinance institutions in Kumasi and Ghana as whole

The implementation of this new IT Audit framework for microfinance and all other small scale financial institutions will serve as a guide in IT Audit and therefore I recommend it for all microfinance institutions in Ghana.

Reference

[1] Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly , 75-105.
[2] Hunton, J., Bryant, S., & Bagranoff, N. (2004). *Core Concepts of Information Technology Auditing*. New Jersey: Wiley.
[3] Kowal, L. (n.d). *COBIT for Internal Auditors.* Retrieved December 13, 2013 from www.nysscpa.org/committees/emergingtech/cobit.ppt
[4] McGladrey & Pullen. (2009). *What is COSO?* Retrieved June 13, 2013 from http://www.mcgladrey.com
[5] Meycor COBIT. (n.d). *Information Assurance Using COBIT.* Retrieved June 12, 2013 from www.datasec-soft.com
[6] National Security Agency. (n.d.). *Defense-In-Depth*. Retrieved March 5, 2013 from www.nsa.gov/ia/_files/support/defenseindepth.pdf
[7] Parkinson, M. (2004). *A Strategy for Providing Assurance*. The Internal Auditor, 63-68

[8] Turcato, L. M. (2006). *Integrating COBIT into the IT Audit Process*. Retrieved June 13, 2013 from www.sfisaca.org

[9] Zhu, A. (2007). *ISMS and Audit Methodology*. Retrieved June 3, 2013 from http://www.docstoc.com/docs/13575720/ISO-27001---ISMS-and-Audit-Methodology