CULTURALLY ALIGNED SECURITY IN BANKING

E. K. KWAA-AIDOO

PhD

UNIVERSITY OF BRADFORD

2010

CULTURALLY ALIGNED SECURITY IN BANKING:

A System for Rural Banking in Ghana

Ephrem Kwaku KWAA-AIDOO

Submitted for the degree of
Doctor of Philosophy

Department of Computing,
School of Computing, Informatics and Media
University of Bradford

2010

Dedication

This thesis is dedicated to my children Yaw Effah and Ama Sroeda and all the people who believe in me.

Ephrem Kwaa-Aidoo
2010

Acknowledgment

First I would like to express my profound gratitude to my research supervisors Dr Andrea Cullen and Dr Rod Fretwell. Without their guidance, wisdom and advice this work would not have come to a fruitful conclusion.

I would also like to express my sincerest appreciation to my brother George Asare-Aidoo who has been extremely supportive throughout the whole period of my study in the UK. I would also like to thank all my friends in Bradford especially in the Catholic Chaplaincy particularly Father Dennis Cassidy and Angela and Anisa for all the support from proof reading my work to offering me a listening ear especially when the going became very tough.

I would also like to thank my parents, Wg. Cdr.(rtd) and Mrs Aidoo, who instilled the quest for knowledge in me.

I would like to thank my family Ama, Yaw Effah and Sroeda for being tolerant and understanding with my being away all these years.

Abstract

This thesis is an investigation into the unique rural banking system in Ghana and the role of information systems in fraud control. It presents a robust information security and internal control model to deal with fraud for the banking system. The rural banking industry has been noted for poor internal control leading to fraud. This has resulted in poor performance and even the collapse of some banks. The Focus of the study was on the processes used to deliver banking services.

To design a protection system, a number of rural banks were visited. This was to understand the environment, regulatory regimes and the structure and banking processes of the industry and banks. Systemic vulnerabilities within the industry which could be exploited for fraud were found. The lack of structures like an address system and unreliable identification documents makes it difficult to use conventional identification processes. Also the lack of adequate controls, small staff numbers and the cross organisational nature of some transactions among other cultural issues reduces the ability to implement transaction controls. Twenty fraud scenarios were derived to illustrate the manifestation of these vulnerabilities.

The rural banking integrity model was developed to deal with these observations. This protection model was developed using existing information security models and banking control mechanisms but incorporating the nature of the rural banking industry and culture of its environment. The fraud protection model was tested against the fraud scenarios and was shown to meet the needs of the rural banking industry in dealing with its systemic vulnerabilities. The proposed community-based identification scheme deals with identification weaknesses as an alternative to conventional identity verification mechanisms. The Transaction Authentication Code uses traditional adinkra symbols. Whilst other mechanisms like the Transaction Verification Code design

internal controls into the banking processes. This deals with various process control weaknesses and avoids human discretion in complying with controls. Object based separation of duties is also introduced as a means of controlling conflicting tasks which could lead to fraud.

Table of Contents

List of Figures

List of Tables

Chapter 1

1 Introduction

Fraud risk has been identified as a major problem in business (Flast, 2009). Banking fraud investigations in Ghana have risen from 25 in 2005 to 130 in 2007 (Editorial Committee, 2008). Ghana's rural banks have not been an exception to this trend in fraud and have had their share of fraud.

Rural banks are said to have weak management coupled with weak internal control systems and non-adherence to uniform accounting guidelines and practices as prescribed in the operational manual for Rural Banks (Coker, 2002). This has resulted in wide-spread embezzlement and fraudulent practices by personnel. In most cases rural banks have no written policies and procedures to guide their operations (CDC Consult Limited, 2009).

This thesis therefore analyses the issue of fraud and presents a fraud control model that deals with fraud risks affecting rural banks.

1.1 Dealing with Rural Banking Fraud

Fraud is an operational risk issue and like most types of risks it is dealt with using conventional risk management techniques. The immediate reaction to the rural banking problem would be to adopt tried and tested banking fraud control mechanisms used in banks the world over. This is however not an option due to the unique nature of the rural banking system and the environment in which it operates. See chapter 2.

Rural banks could also use widely accepted risk management techniques for identifying risks, quantifying them and adopting bespoke cost effective mitigation mechanism. Using this method however would be problematic mainly because of the approach normally used to quantify risk. This approach estimates risk as a product of the likelihood of a fraud and the exposure to it. It requires knowing the likelihood of risks and the exposure should the risk occur. Data indicating the likelihood of risk events occurring is however not available in the rural banking industry. This leaves the option of depending on the intuition of risk managers in assessing the likelihood and exposure of occurrence of adverse events. This approach is highly subjective and unreliable as a means of choosing what risks to mitigate and how to mitigate it.

1.2 Contribution

A key contribution of this research is the Rural Banking Integrity Model (RBIM). This is a fraud control model that is designed to meet the needs of the rural banking industry. In this model identity is seen as a social construct. Personal identity is presented in terms of personality and individuality and as an integral part of a social identity. This paradigm is presented as an alternative to the current means of identification where

people are identified through personal identifiable information linked to inanimate objects like an address or an identification document.

Also presented in the model is the use of traditional Adinkra symbols for authentication. In addition a set of transaction controls are integrated into the business delivery processes. These controls are designed in such a way that it ties the physical elements of the banking processes to records representing them. They are also designed in such a way that they cannot be bypassed in an attempt to commit fraud.

The thesis also contributes to the understanding of the interrelation of culture and security. Most security models involve a set of secure states and the transition rules that allow them to move from one secure state to another. They are however generic and appear to be value neutral. In an attempt to implement part or a combination of these models there is the need to take into account the context of the environment into which they would be implemented. This thesis adds to the understanding of the inculturation of security models. Although the RBIM is mainly based on the role based access control and the Clark – Wilson models, it takes into account the context of the rural banking industry. This is done by aligning control mechanisms to the traditional culture and the goals of the various stakeholders of the industry. This alignment is seen especially in its transition rules.

1.3 Broad Aims

The basic premise of this thesis was to look for ways to design an effective internal control model to deal with the problems in the rural banking sector mentioned above. This research took a holistic view of rural banking in Ghana in the process of designing

mitigation mechanisms. This approach was adopted because rural banks are unique in nature as a result of the laws that create and regulate them.

Various characteristics set rural banks apart from any other bank. Key among them is that they operate in rural Ghana and are limited by law in their geographical area of operation hence simple transactions become cross-organisational with its associated problems. In addition the banks are small units and therefore do not have the resources available to large commercial and investment banks.

The rural banking industry is in the process of computerisation and there are plans to implement computer systems throughout the entire industry (Editorial Committee, 2005). Information stored on such a system would represent the resources and customer deposits of the bank. Arbitrary changes to such data can result in the loss of these resources. Criminals could target these systems to appropriate corporate resources to themselves. With information security techniques being the means by which computer systems can be controlled it become the prime means for controlling rural banking business processes.

In this thesis, there is a shift in the view of the role of information security. Traditionally information security is seen as a way of dealing with risks that arise as a result of the use of technology and is therefore used to protect information systems from posing risks to businesses. Information security systems become a self serving exercise which is deployed to protect the information system rather than the business. The view of information security in this thesis is to expand its use from protecting information systems to protecting the business as a whole by reducing business risk. Information security is therefore used as a risk management tool.

The approach used to achieve an effective security design in this thesis involved an analysis of the nature of the industry, the environment within which it operates and the business processes used to deliver services to the public.

The focus of the analysis was to thoroughly understand the rural banking industry. The analysis also identified vulnerabilities in the industry and the threats that were present. In addition it also identified the enabling conditions and the opportunities presented within the industry and the environment for the implementation of controls.

Two main problems were found in the study. The first were problems with the identity management of both customer and staff. The second had to do with problems with the internal control mechanisms that were used to deal with transaction failures. Threats to the system it was observed came from both customers and staff who used deception for personal gain.

To deal with this requires that data objects must only be modified by authorised people in authorised ways. In this regard, the proposed model deals more with data integrity issues than confidentiality. Though Confidentiality is desired, commercial security concerns have always had integrity of data as their prime objective (Clark and Wilson, 1987) and in this case seems more appropriate. The rural banking system was therefore designed to ensure that the integrity of data is maintained.

The rural banking integrity model is presented as a fraud control model designed to meet the needs of the rural banking industry. It combines various mechanisms to create a generic model for the protection of the rural banking system. It adopts mechanisms from information security models like the Clark-Wilson model which is developed

based on traditional business controls like the double entry system. It also uses traditional culture and practices of the communities within which the banks operate.

The proposed system is presented as a generic rural banking fraud control model. It could be adopted in full or in part to deal with fraud depending on the priorities of security managers and on the circumstances of the implementing bank.

1.4 Objectives and Research Questions

The objective of this research work was to develop model using access control techniques for the purpose of improving fraud control within rural banks. It was also an objective to take a broad view during analysis and design to identify and consider all factors which might not be traditionally considered in risk management and security system design.

The specific objectives were to:

1. Analyse the business process used to deliver rural banking services and to determine the vulnerabilities associated with these processes. This analysis looked at:

    a) What controls were used to prevent fraud and how reliable existing controls were,
    b) The extent to which these controls were being adhered to and
    c) How banking operations could be made more secure especially against fraud.

2. Analyse the rural banking industry and the environment it operates in to identify the factors that could influence fraud control either positively or negatively.

3. Examine the possibility of the use of information security technology particularly access control techniques to enhance fraud control. An emphasis was to look at the design of transactions and the introduction of control mechanisms with special emphasis on:

    a) Roles,
    b) Conflict of interest and the risks they create
    c) Separation of duties as a control mechanism
    d) The existing environmental conditions that can be taken advantage of to create a reliable and suitable security system that could enhance fraud prevention and control.

These objectives led to the following research questions that were answered:

1. Can conventional banking controls used by banks all over the world be applied to the rural banking industry to safeguard it against fraud and operational risks?
2. In what form could role based access control techniques be implemented within the rural banking system to support internal control of banking operations to give reasonable assurance against fraud through the:
    a. Control of possible overlap of functions/permissions of members that can create potentially dangerous conflict of interest situations and the opportunity for fraud in the rural banking system.
    b. The design of transactional processes and the incorporation of security requirements into transaction functions.
3. In what way could internal control mechanisms be enforced to prevent the users having an option not to adhere to controls?

4. How can the identity of customers and employees be managed in the rural banking system to prevent fraud?
5. To what extent could the socio cultural characteristics of rural Ghana be tapped and used for engineering security to solve operational risk issues in general and fraud in particular?

1.5 Methodology

Various methods were used to collect and analyse data to help arrive at the conclusions and to design the threat mitigation mechanisms in the security model. A diagram showing the methodology is shown in figure 1.1.

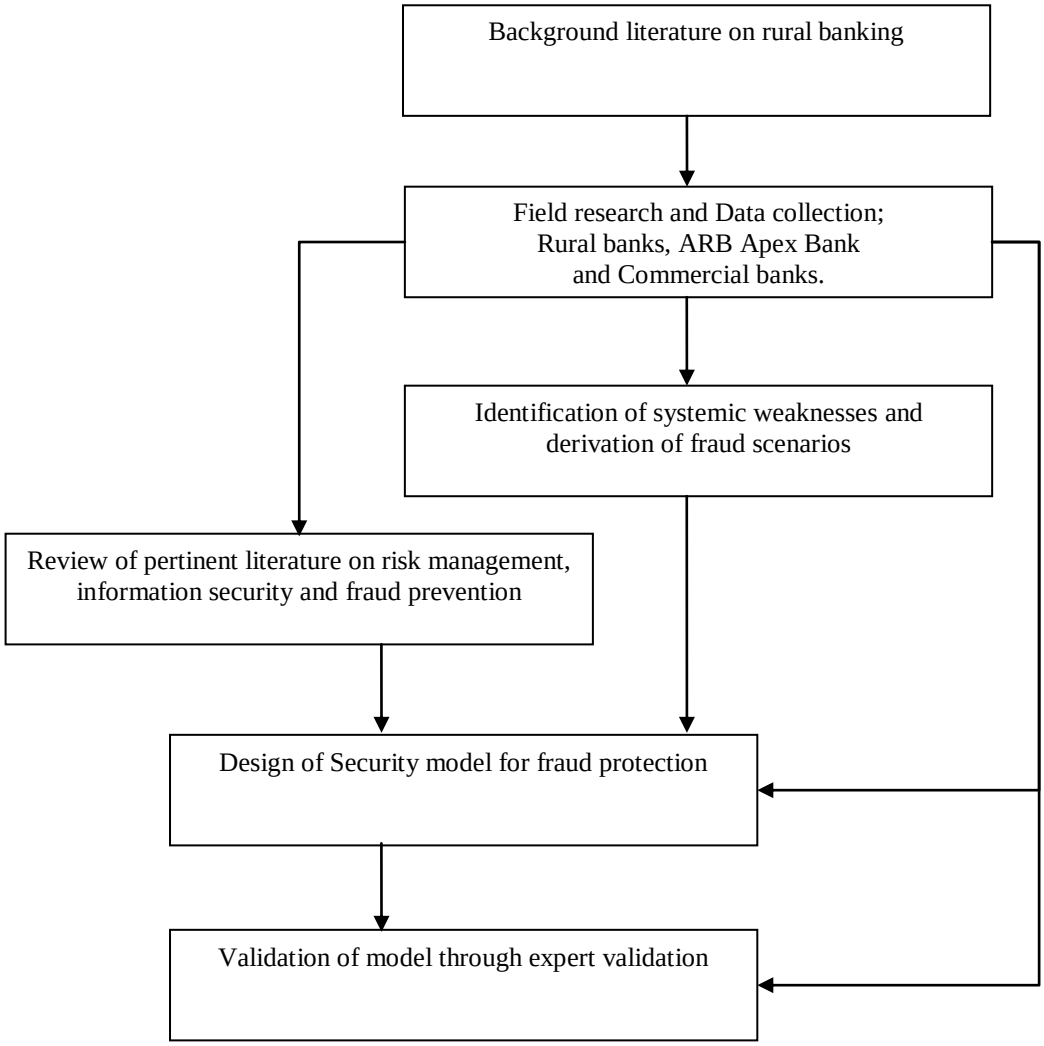


Figure 1.1 Methodology

1.5.1 Review of Relevant Literature

Initial background work was done to understand the nature of the rural banking industry to help understand the industry. This initial search helped shape the field research that followed. Issues to do with the characteristics, regulatory regime, and location of rural banks among other issues were looked at. It also helped to shape the type of information to be collected and from whom to collect.

The nature and the different type of risks and their treatment were looked at. Security concepts, goals and techniques were also examined. Well known security models including role based access control, the Clark-Wilson, Chinese wall and others like the role based access controls frame work was also examined to see how they could be applied to the problems identified during the field work.

1.5.2 Field Research

Data collection was done through a field research. It was the chosen because it offered a better means to understanding the nuances of the issues within the rural banking system. It was seen as the most effective means of understanding the details of what is done in the daily operations in rural banks. It gave the opportunity to identify new information. This was very important since there is little research into the operations of rural banking.

The data collection methods used during the field research included a structured questionnaire, observation and interviews. Documents were also studied.

Data collected included the structure of the banking industry and the individual banks. Detailed information on the services offered by the rural banks was also collected during the field work. A systematic description of the processes used to deliver the services was done. Process controls in use within the rural banks were also documented. Another important part of the field research was to understand the nature of the communities that the banks operate in.

Vulnerabilities within the systems and processes were identified and documented. This was done through discussions and interviews with employees and banking professionals and also from reported incidents.

The views of the rural and other commercial banking operations were also collected with regards to the level of effectiveness of controls and the possible means by which these controls can be improved.

1.5.3 Derivation of scenarios

After documenting banking processes and collecting other information on rural banking systems vulnerabilities or systemic weaknesses were identified. The possible manifestation of systemic weaknesses or vulnerabilities within the banking processes was then identified. These were documented in the form of twenty fraud scenarios built as an illustration of the vulnerabilities within the system. The scenarios were either fraud cases that had occurred within the rural banking or commercial banking systems or incidents that could occur. They were derived during the field research and were discussed with the banking officials to confirm that they could actually happen given the weaknesses.

1.5.4 Design of security model

A comprehensive security model was then designed for the protection of the rural banking industry against fraud at this stage. This was based on the risk and security techniques examined and the views of banking professionals interviewed during the field work.

1.6 Organisation of write up

This thesis consists of nine chapters the remainder of which is organised as follows;

The second chapter looks at the background literature of rural banking in Ghana, the nature of risk, operational risk and fraud. Chapter three discusses the management of risk within business and the banking industry. It also proposes internal controls

enforced using information security mechanism as the best means for dealing with it. A discussion of the techniques available to achieve the various fraud control objectives is done.

Chapter four discusses the interaction of security and culture. It takes particular look at the culture of Ghana and how it might influence security management. Chapter five presents the methodology that was used in the study.

A presentation and discussion of the information obtained from the field research is presented in chapter six. The identified threats and the vulnerabilities identified in the field research are also discussed in this chapter. The Seventh chapter discusses twenty fraud scenarios and their variants obtained from the field studies and derived from the analysis of the data obtained from the field research.

The eighth chapter discusses the Rural Banking Integrity model which is a system design aimed at the mitigation of the risks identified during the field studies. The ninth chapter presents conclusions and future work.

Chapter 2

2 Rural Banking and the Issue of Fraud

This chapter introduces the rural banking industry and discusses the unique points of the industry that could potentially create fraud risks. It discusses some of the conditions created by the regulations that govern rural banking industry and its impact on risks. It next explores the issue of risks in general and operational risks in particular focusing on the nature of fraud. It classifies fraud into four main types and then discusses the conditions that enable fraud.

2.1 Rural Banking within the Banking System

Rural banks are commercial banks with restrictions on what services they can offer and where they can operate (Andah, 2005). This banking system was created to provide banking services to the rural Ghanaian population who most often do not have any form of financial intermediation.

According to the bank of Ghana, banks are divided into three main tiers in Ghana (Editorial Committee, 2008) as shown in figure 2.1.

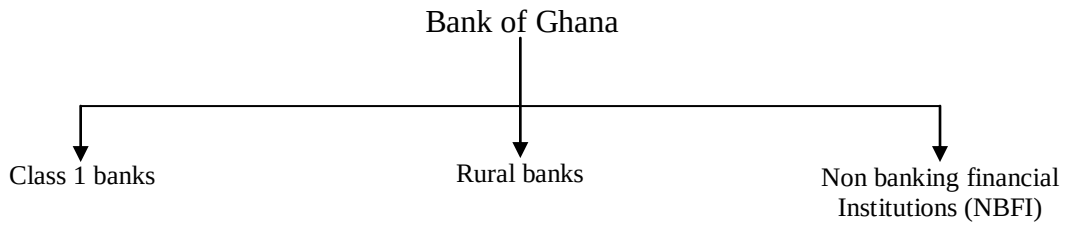


Figure 2.1 Structure of the Ghanaian banking industry

The bank of Ghana reported a total of 126 rural banks in their 2007 annual report forming one of the tiers of banking. The other tiers are 23 main stream commercial banks also known as class 1 banks and 42 Non Banking Financial Institutions (NBFI). Generally the main stream commercial banks and rural banks are separated from rural banks by their capital requirements and the scope of business activity.

2.2 The Nature of Rural Banking

A look at rural banks shows an industry closely interlinked to the communities they operate in. It also shows that they use alternative mechanisms which could be effective.

There are currently 135 registered rural banks operating in various parts of Ghana at the end of June 2009 which is an increase of 9 banks from the 2007 figure.

Region	No. of Banks
Ashanti	25
Eastern	22
Central	21
Brong-Ahafo	21
Western	14
Volta	11
Greater Accra	6
Upper East	5
Upper West	4
Northern	6
Total	**135**

Table 2.1 Distribution of Rural Banks (Bank of Ghana, 2009)

Table 2.1 shows the regional distribution of rural banks. Rural banks have branches and these are referred to as agencies. The ARB Apex bank reports a total of 439 agencies (ARB Apex Bank, 2008). Rural banks are limited liability companies with their main source of funds for operations (especially loans to customers) being government and international grants and loans. They are owned by the communities within which they operate with the Bank of Ghana having preferential shares.

Rural banks are essentially community banks often referred to as such by the bank of Ghana. Their operations are however limited to rural Ghana. They are therefore meant to have close relationships with the communities they operate in. Community banks generally aim to help keep local communities vibrant and growing (Independent Community Bankers of America, 2009). They focus their services to their localities and in doing so, community banks have the unique advantage of understanding the locality and clientele much better than large commercial banks do.

Rural and Community banking was started in 1976 when it became clear that main stream commercial banks were not meeting the microfinance needs of the rural people in Ghana (Essel and Newsome, 2000). The focus of their activities is therefore not

solely commercial but also developmental. They focus their attention on the needs of local families, businesses, and farmers. Like community banks around the world, rural bank officials are usually accessible to their client with most officials having close physical, social and emotional involvement in the local communities. Since community banks are themselves small businesses, they understand the needs of small business owners who form the bulk of their clientele.

Rural banks are meant to operate like traditional community banks taking deposits and lending it back but in this case to the same communities where depositors live and work (Community Bankers of Wisconson, 2009). Large commercial banks are however structured to place a priority on serving large corporations and less intimate urban clientele. Unlike community banks, large commercial banks move deposits from one community to lend to another community.

The other unique characteristic of community banks is that they use very intimate methods in the provision of their services and tend to know their customers. Even in advanced countries like the United States, community banks are likely and willing to consider character, family history and discretionary spending in making loans (Independent Community Bankers of America, 2009). This is in sharp contrast to large commercial banks who often apply impersonal qualification criteria, such as credit scoring to all loan decisions without regard to individual circumstances. Community banks are also reputed to offer nimble decision-making on business loans. This is because decisions are made locally as opposed to using loan approval committees who do not have the benefit of local knowledge. It is also worth noting however that many commercial banks are introducing some elements of customer relationship banking to get to know customers for the purpose of introducing some form of customisation of

services and risk rating. This is an indication of the credibility of methods employed by organisations like community banks to deliver their services to their clientele.

Though rural banks share a lot of similarities with other banking institutions, they have many characteristics that make them very unique. Various factors account for the unique nature of rural banks. Key among the factors is that the legislation that creates rural banks put various restrictions on them. These restrictions have resulted in creating unique operating conditions very different from all the other financial institutions in the country. The main restrictions put on rural banks are the type of services they can offer, their area of operation (catchment area) and capital requirement. The effects of these are discussed below.

2.2.1 Banking Law and Rural bank's Catchment Area

Restrictions on rural banks limit the extent of their operations and this has an impact on their size and the security of operations. Rural banks operate as commercial banks under the banking law, Act 673 and its amendment Act 738, except that they cannot undertake foreign exchange operations and their clientele is drawn from their local catchment area (Andah and Steel, 2003). They therefore accept deposits and offer lending to their clientele.

Rural banks are also allowed a 20 mile radius as their rural catchment area and are not permitted to operate outside this catchment area. They cannot therefore open branches in different localities outside the catchment area which they have been authorised to operate in. Due to the restriction placed on their area of operation, a transaction that has parties beyond their catchment area has to involve another organisation or bank to deliver the one end of the transaction. One of the main parties is usually the ARB Apex bank which was created to provide such services.

Though rural banks are not limited in the number of branches they can operate within their catchment area, there are so many branches they can operate to make business sense. This situation could be a severe barrier to their growth especially when they operate in poor rural communities.

2.2.2 Characteristics of Rural Ghanaian Communities

Rural banks operate in unique environment. As mentioned earlier the rural banking concept was created to provide banking services to rural communities they are therefore limited to operating mainly in rural areas. The Ghanaian government defines "rural" to be a village of 5,000 inhabitants or less (Essel and Newsome, 2000). The nature of rural communities has a huge influence on the operations of the banks due to the character of the rural folk and the lack of access to technology. Rural Ghana is by and large 100% African and has various traditional and cultural characteristics that are very different from other cultures and have unique characteristics unlike many communities around the world. These include family cohesion and community identity and is characterised by high illiteracy which has various implications in implementing business protection mechanisms. These are discussed in Chapter 4.

Rural population of Ghana forms about 63% of the country's population (IFAD, 2007). It is characterized by a largely agricultural economy, high levels of poverty contributing about 90% of national poverty (Yeboah, 2007) and high illiteracy level of 62% (Aryeetey and Kwakye, 2005). With such characteristics of the population, solutions involving cutting edge technology and that require human interventions and or formal education could be a problem to implement and is unlikely to be successful.

For rural banks, the nature of the rural community could present opportunities and threats in the management of organisational risks. This is because human beings are

very easily conditioned to accept the social framework around them as though it was a part of the natural world, and therefore no more under their control than the weather (Hilder, 1995). Most rural folk could accept family norms and practices without question. In designing control mechanisms it becomes crucial that the nature and character of the communities are understood in order to develop or adopt mechanisms that can work under those circumstances.

2.2.3 The Paradox of Rural Bank Regulation

Rural banks are regulated by the ARB Apex bank which presents a regulatory paradox as would be seen shortly. This could have an impact on fraud control. The primary need for regulating financial institutions is the protection of public depositors in financial institutions (J. Gallardo. 2002). This is a result of conflict of interest between the bank seeking its own interest and that of its customers. Hence the need for an impartial third party usually the state or an agency of the state. The state's interest is usually in sustaining the integrity of the whole of the sector and this also attracts the interest of the state to the entire payment system.

The regulatory framework usually defines the regulatory authorities and the scope of business in terms of their products. It also defines the entry and exit requirements and most importantly standards of sound operation of the business in order to ensure sustainability.

Regulations of financial institutions are usually in two forms: prudential and non prudential regulation. According to Christen et al (2003) prudential regulation is aimed specifically at protecting the financial system as a whole as well as protecting the safety of small deposits therefore, it involves the government overseeing the financial soundness of the regulated institutions.

Non-Prudential regulation relevant to Microfinance span a wide spectrum and Christen et al (2003) indicates that they include enabling the formation and operation of microfinance institutions, protecting customers, preventing fraud and financial crimes and setting up credit information services. It also supports secure transactions and also develops policies with respect to interest rates, setting limitation with respect to foreign ownership, management and source of capital and identifying tax and accounting issues. Most of these are done by the banks themselves.

The Bank of Ghana is mandated by law to regulate banking and non banking financial institutions. Rural banks are therefore ultimately regulated and supervised by the Bank of Ghana. Andah (2005) indicates that the regulatory process of Bank of Ghana is based on the type of institution rather than the type of transaction. The implication is that rural banks have a different regulatory from that of the main stream banks.

Rural banks are regulated by the ARB Apex bank as mentioned earlier. Association of rural banking (ARB) in 2001 set up the ARB Apex bank. The purpose of the bank was promotion, check clearing, specie movement, treasury management, training and product development. The Bank of Ghana has however ceded regulation of rural banks to the ARB Apex bank. The bank of Ghana however remains the main regulator of all financial institutions in Ghana. The paradox in this structure is that the ARB Apex bank exercises control over its owners. There is the likelihood that ARB Apex bank would seek to satisfy the state which requires prudential regulation to maintain the integrity of the financial system since the state also supervise it. On the other hand they could be soft on non prudential regulation because it is not the priority of the state and management of rural banks might not want to cede such control to a bank they own.

This puts more responsibility on the banks and the creation systems that could remove the weaknesses in controls which could result from this regulatory regime.

2.2.4 Capital Requirement and the Nature of Rural Banks

Rural banks are generally small banks set up with a small amount of capital. This is partly a result of the low capitalization requirements of rural banks which has led to the small sized operations of rural banks. This limits the ability of the banks to undertake an extensive IT and risk management programs.

The minimum capitalization requirement for a rural banking license is 150,000Gh Cedis (Banking Supervision Division, 2006), about $150,000 which is significantly lower than that required for class 1 commercial banks. The Bank of Ghana's licensing requirements for main stream banks is 60millionGh Cedis (Banking Supervision Division, 2005) the equivalent of $60 million and about 400 times the requirements for a rural bank. Of the capital requirement of rural banks, ownership by corporate bodies should not exceed 50% and individuals not exceed 30%. (Jha et al., 2004 , BoG, 2006).

Though there are some relatively big rural banks, they are generally small businesses with low level of technology usage mainly because they do not have the financial resources to implement big computerization projects. The solution to the lack of technology has been to implement a government sponsored information technology systems projects under the Apex bank. In 2006 the Millennium Development Authority announced a $20 million Ghana Rural Bank Computerisation & Interconnectivity Project (GRBCIP) under the Millennium Challenge Account (Editorial Committee, 2009). This is to automate the accounting system of most rural banks using a common software platform. I will link them in a wide area network under the Apex bank to

further integrate them into the economy and offer better savings, credit and cash transfer services to the rural population.

The new system would create a distributed system linking autonomous organisations. Laudable as this project is, it raises several issues to do with information security risks, fraud and operational risks. Key among them is the issue of who has control over what information. If information is being transferred from one bank to another the question of where the responsibility of one bank ends and another starts arises. The new system is also bound to be more susceptible to increased fraud because of the increased ease and speed of money transfer between rural banks. There is therefore the urgent need to understand the nature of rural banking industry, the risks they face and to urgently design and implement control measures to mitigate them.

2.3 Risks and its Manifestation in Banking

It is important to understand the nature risks faced by businesses in order to develop mitigation systems. This is more so when there are varied risks in banking. Risk is described as the uncertainty with an exposure to loss, the undesired, unplanned, reduction of economic value (Tung-Chien, 1987) alternatively it has been described as the exposure to a proposition for which the outcome is uncertain (Holton, 2004). Risk, no matter the context refers to the possibility of suffering loss and this invariably refers to a probability of impending danger. The issue of risk in business is not about the existence of risk but rather what is to be done about the risky situation. Risk management therefore defines the discipline of balancing the opportunities you seek against the loss you wish to avoid (Alberts and Dorofee, 2005). Closely associated with business operations are risks which prevent business organisations from attaining their business goals. Conventionally risk is estimated as a measure of two components.

These are exposure and uncertainty which are both required for there to be risk. Uncertainty is the likelihood of the risk event occurring and exposure the amount of loss that could potentially occur.

Today's banking systems are heavily dependent on complex computer based information for majority of their services and it is critical to ensure optimum security protection to ensure that strategic goals are attained. Rural banks would self destruct together with their goals of using financial intermediation as a tool for development if identification of risks is not done and the subsequent translation of these risks into a set of mitigating systems to manage them.

In banking risk is manifest in various ways it could be customers defaulting on loans, or an investment resulting in a loss. On the other hand banks could suffer a loss as a result of a lawsuit, loss of reputation, errors and fraud among others. Normally banks classify risks into three main categories (Eccles et al., 2001). These are market risk, credit risk, and operational risk.

Market risk refers to the uncertainty of future earnings due to changes in the value of financial instruments caused by movements in market parameters. Credit risk refers to the uncertainty of loss that may arise as a result of obligators mostly borrowers failing to meet the terms of a financial contract or otherwise failing to perform as agreed. Operational risk on the other hand refers to the possibility of loss as a result of human error, management, or deficiencies in the operational systems (Eccles et al., 2001). Market and credit risks are transaction based in other words they depend on or differ from transaction to transaction whereas operational risk on the other hand is systemic (Mainelli, 2002 , Thirlwell, 2002).

2.4 Operational Risks in Banking

Operational risks are rare and highly varied. The Bank for International Settlement's Basel Committee(BCBS) in a document supporting the new capital accord defines operational risk as the direct or indirect loss resulting from failed internal processes, people and systems or from external events (Basel Committee on Banking Supervision, 2001). It is worth noting that various organisations and authorities have given different definitions of operational risk. A popular description of operational risk refers to it as every risk source that lies outside the areas covered by market risk and credit risk (Jameson, 1998). Operational risk has also been defined as the uncertainty of loss in the book value of the firm due to failures in the manufacturing of the firm's goods and services (King, 1998). The second definition in particular gives an indication of the varied nature of operational risks.

In banking however the definition by the Basel committee seems to have widespread use. The Basel Committee further defines seven activities that fall under operational risk. These activities are:

i. Internal Fraud
ii. External Fraud
iii. Activities relating to client products and business practices.
iv. Damage to physical assets
v. Business disruption and systems failure
vi. Execution delivery and process management (Basel Committee on Banking Supervision, 2001)

Operational risk problems that have surfaced in banking institutions like Barings bank, Daiwa bank, Sumitomo, and National Westminster Bank (Thirlwell, 2002) not to

mention the 2008 Société General Bank rogue trading problems have shown the significance of operational risks management to the survival of banks. Though the mechanism used to perpetrate each of the fraud is different, the underlying cause is the failure of the banks procedure to deal with the risks, the lack of adequate controls processes or the inadequate enforcement of control processes leading to huge losses. Economic factors are frequently blamed for several banking crises whilst the real problem comes from the banks' own strategies or operations. Unauthorised transactions associated with the failure of internal controls appears to have increasingly become the major source of bank losses as shown in the cases of Barings, Jardine Fleming, Morgan Grenfell and Daiwa. All these loses have been linked to either a deficient organisational structure inadequate, poor recording and audit trails and Lack of controls and verification (Holton, 1996). The rest include the lack of proper audit arrangements coupled with the deficient understanding of the systems; conditions that have presented an opportunity for fraud. Needless to say the problems above had nothing to do with credit worthiness of customers or market fluctuations but a failure to control activities of employees and the banking processes.

As shown by the range of activities that could result in operational risks, the range of losses is very wide and they can be a direct or indirect result of failure of internal processes. The direct impact of failures ultimately results in the loss of bank assets.

Find below examples of direct financial losses attributed to operational risk failures between November 1995 and March 1997. Since then there have been other high profile cases notable is the 2008 Société General trading loss costing 4.9 billion euro (Arnold et al., 2008). It is well worth noting that all of these frauds were perpetrated by internal operatives.

Date	Type of firm	Loss (USD)	Brief Description of allegation
Nov – 95	Bank	4 million	Computer problems with Fed payment connection
Feb – 93	Corporate	1.04 billion	Unauthorized futures trading
Apr – 94	Brokerage firm	350 million	False profits reported for two years
Sep – 95	Bank	1.1 billion	30,000 unauthorized trades over 11 years
Feb – 96	Bank	1.3 billion	Losses from NIKKEI futures hidden in 88888 account
Jun – 96	Bank	1.8 billion	Unauthorized copper trading – futures, etc.
Aug – 96	Fund	19.3 million	Deal allocations delayed for personal profit
Sept – 96	Bank	750 million	Dummy companies used to avoid compliance
Mar – 97	Bank	130 million	Option volatilities used to inflate prices
Mar – 97	Bank	100 million	Funds transfer to personal account

Table 2.2 Example of financial loss attributed to operational risk (King, 1998)

Indirect losses on the other hand could be in the form of reputational risk resulting loss of confidence in the bank as a consequence of operational risks. Legal risk could also arise resulting in fines, criminal liabilities and special penalties being imposed by supervisors and regulators. In reality credit and market risk could be affected by operational risk.

As indicated by the Basel committee in their definition of operational risk, threats could come from both internal and external sources. However due to the proximity of internal operatives to the system and their familiarity with it they tend to be more of a threat and indeed threaten the system more than outsiders. Although external fraudsters, Hackers and virus attacks are well publicized, the insider remains the greatest threat to an organisation in terms of potential to cause financial loss (Small, 2004). This is clearly shown by the notable fraud cases in table 2.2. Unlike fifty years ago when it was difficult for a single employee to bring down an entire multinational company, it has happened too often now and could easily happen again.

The risk of internal operatives notwithstanding, all other forms of threats should not under any circumstances be underestimated especially since a single incidence of fraud

or security breach could cost a bank several millions of dollars and could eventually lead to its collapse.

Due to advances in technology especially manifested in computer networking particularly in the form of the internet and distributed systems, various business processes have been linked together in complex interrelations. E-commerce has arisen out of these technological innovations and has created distributed work processes that cuts across organisation boundaries. Typically no one has end to end management authority in a distributed work process, which makes risk assessment and management an extremely difficult proposition in these environment (Alberts and Dorofee, 2005). Such is the model which is expected to be created by the proposed extranet based system for Rural banking system which would be used to run services like the Apex link (local money transfer scheme). In such a system no single rural bank or the ARB Apex bank would be able to have complete control of certain types of transactions. This scenario creates a complex risk environment considering the current operational risk problems of the rural banking system.

2.5 The Nature of Fraud

Fraud is a major form of operational risk and is hence rare and varied. It has been described as a moving target and that its control is highly dynamic (FORE, 2005). This is because of the varied forms in which they are manifest and because fraudsters always devise new methods when old methods cease to work. It is therefore difficult to extrapolate past fraud cases as a means of predicting future fraud situations. It is rather more important to thoroughly understand the issues surrounding fraud and its patterns in order to prevent it. Organisations should be thoroughly understood in order for good anti-fraud measures to be designed and implemented.

The Oxford English Dictionary defines fraud as criminal deception intended to gain money or personal advantage (Oxford University Press, 2002). Lanza (2003) refers to fraud as all multifarious means which human ingenuity can devise, and are resorted to by one individual to get an advantage over by false suggestion or by suppression of the truth. As is indicated in the definitions, the key action to committing fraud is the use of deception for the purpose of personal gain leading to a loss to the firm or another person. It includes surprise, tricks, cunningness or dissemblance and any unfair way in which another is cheated. Occupational fraud refers to a case where an organisations falls victim to its own member, has also been defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisation's resources or assets (Lanza, 2003).

The indication from the above definition is that fraud could be from internal or external sources however about 69% of frauds are perpetrated by an inside fraudster with another 20% being collusion between and insider and outsider (KPMG, 2007). This makes the insider the biggest perpetrator of fraud. One of the main reasons for this is that the insider understands the organisations systems and hence able to spot and exploit any weaknesses and also because they have physical access to systems which is often poorly managed (Wilson, 2005).

Generally for a fraud to occur, an individual or an organisation intentionally makes an untrue representation about an important fact or event. The untrue representation is believed by the victim be it a person or organisation to whom the representation has been made. The victim relies upon and acts upon the untrue representation and suffers loss of money and/or property as a result of relying upon and acting upon the untrue representation. Fraud operates in a paradigm where deception induces the victim to act

to their own detriment and to the fraudsters benefit (Doig, 2006). Deception is therefore critical to fraud and without it fraud cannot occur. The difference between conventional theft and fraud is that while the perpetrator uses threat of violence or intimidation to coerce the victim to hand over property in conventional theft, fraud uses deception and misrepresentation through words or documents.

Generally fraud has often been classified based on what the victim was buying or what medium was used for the transaction that the fraud occurred in. So fraud is classified into many groups like credit card fraud, benefit fraud, dance instruction fraud, internet fraud etc. This description does not ensure a proper understanding of these fraud types. Fraud has been classified as an operational risk and therefore the process used to perpetrate the deception should be a more appropriate as a means of describing it. When the focus is put on the deception process used, they seem to come in a few forms. Below is an analysis of some of the notable fraud instances and the patterns they seem to follow.

2.5.1 Deception by Adopting an Identity

In a fraud case a customer of United Mizrahi bank Philip Ashley in the UK wanted loans amount for his company which was in excess of the bank's loan limit. He therefore set up different shell companies which he used to apply for separate loans which were individually below the bank's loan limit but to the tune of £3.7 million in total (Office, 2003). He was only found out when the companies went bankrupt. In fraud cases of this type the fraudster hides his real identity or adopts another person's identity to gain a status of a "genuine customer" for which he uses to request for transactions. In this case you have an imposter gaining genuine banking authority that allows them to request transactions. In this case of Philip Ashley for example the bank

was not able to match the real identity of the person behind the company to the natural person. The ability to match the identity on the bank's records to a natural person becomes very important.

2.5.2 Fraudster Assuming Forged Authority

In this type of fraud you have a non customer who has been authorised in many instances to perform transactions on behalf of the customer using forged documents and signature to perform a fraudulent transaction. A notable example of this type of fraud was committed by Joyti De-Laurey who has been described as Britain's biggest female fraudster. De-Laurey, a secretary at Goldman Sachs used access to her boss's cheque books and signature and the fact that she had to perform such transactions for him to steal up to £4.3 million from his account (Harding, 2004).

In this type of fraud the perpetrator though not the account holder was seen as acting on behalf of his boss and with access to genuine documents performed fraudulent transactions. Though she had been authorised to perform many transactions on behalf of her boss she obviously did not have the authority to perform the fraudulent transactions but was able to pass herself off as an authorised actor in that instance. Obviously the bank was not able to detect when she had genuine authority and when she did not. In this case it is important to be able to verify that a customer has authorised a transaction especially when it is being requested by another person.

2.5.3 Unauthorised Transaction

There are also fraud cases where an authorised person, usually an insider, perform what is seemingly a normal transaction but for their own benefit. Here you find an authorised person using a genuine document performing an unauthorised transaction. A case is one where Mel smith deputy director of the finance department of the Metropolitan Police

committed a £5 million fraud (Doig, 2006). Smith was in charge of the ordering and dispensing fund for the informant and covert work relating to terrorism in 1986. Due to the level of secrecy and the faith of the department in him he was able to withdraw monies from the fund for his personal use. In this type of fraud the perpetrator is in a responsible position and authorised to perform these transactions however he uses this authority to deceive his organisation performing transactions that were rather to his benefit.

In this type of fraud you can find employees put in positions of trust performing unauthorised transactions to benefit themselves.

2.5.4 Trust Based Fraud

This type of fraud is based on the trust the victim has for the perpetrator. This enables the victim to hand over money and other valuables to the perpetrator on trust. One form of this type of fraud is investment fraud. It arises when a seemingly lucrative business proposal is made to be invested in. It could be in the form of a pyramid scheme as was perpetrated by Bernard Madoff (Clark, 2008 , British Broadcasting Corporation, 2008) or the Salvation Army /Stuart Ford £6.6 million fraud (Doig, 2006). The former described as the biggest financial scandal in the history of markets, Bernard Madoff set up a company and took the money belonging to investors to the tune of £33 Billion and just run a ponsi/pyramid scheme where he paid returns from their own money or from subsequent investors.

In the latter Stuart Ford took £6.6 million from the Salvation Army and sent it to banks around many countries claiming to be investing it for them. Of the £6.6 Million he paid £200,000 to the Salvation Army. In all the cases supposedly reputable investors presented investment proposals to investors and took their money.

Another form of this fraud is the 419 advance fee fraud named after the section of the Nigerian criminal code which made such activities a criminal offense. It originally focused on gaining the victims account details to execute a fraud against the account. However recent cases seem to focus on convincing the victim to make an advance payment to facilitate a transaction that would enable them to share in a large sum of money (Doig, 2006). This type of fraud is used in many instances. An example is the corporate advances /peninsula holdings fraud case. In this case, an advance due diligence fee of between £25,000 to £50,000 was paid to Peninsular holdings after a £6-7,000 fee was paid to Corporate Advances before being referred to Peninsular holdings (Ramage, 2005). As with all fraud there is a relationship that is built between the victim and the perpetrator. This type of fraud takes advantage of the trust in the relationship request a fee which commits the victim to the deal and further makes them susceptible to more demands of payments. It is not very likely for banks to suffer this form of fraud.

Other forms of this type of fraud arise when a victim is conned based on trust into entering a fraudulent contract or agreement which only benefits the perpetrator.

In all the various types of fraud, a perpetrator acquires a trusted profile that enables them to conduct some transactions with the victim. This might involve the acquisition of a new/fake identity to enable this profile to be created or pretending to have the authority to do that they don't have. When the perpetrator already has a trust profile to request a fraudulent transaction, certain documents might be necessary to enable the fraud. This could be forged if genuine ones are unavailable. Then with the profile and the relevant documentation a transaction could then be requested. What is however

common among these fraud instances is the lack of controls that made the deception possible (Doig, 2006).

From the preceding it shows that to detect or prevent fraud there must be controls that can reliably match an identity to a natural person and verify reputation, verify that documentation and verify authority to perform the requested transaction.

2.5.5 Profile of a Fraudster

It is very difficult to profile a fraudster because their known characteristics seem to fit many people. An example is Jerome Kerviel the perpetrator of the 2008 Societe Generale €4.9 million fraud. He has often been described as a low level trader who did not distinguish himself from others with no hint of glamour or brilliance (Carvajal and Brothers, 2008).

A KPMG survey of fraud in Europe, India, Middle East and Africa found that most fraudsters seem to be ordinary at first glance because they are generally seen to be helpful, polite and inconspicuous and most importantly are colleagues that enjoy the absolute trust of both colleagues and superiors (KPMG, 2007). The report however found that in about 85% of cases, fraudsters were males with 70% between the ages of 36 and 55 years acting alone 68% of the time. Most fraudsters were long time employees or the organisation with 36% having worked for the company 2-5 years and 22% working for the organisation for more than 10 years. This makes it very difficult to profile a fraudster based on the fact that there are many ordinary, trustworthy male colleagues who can easily fit the description.

Cressey's Fraud triangle refers to three elements present in every fraud. These are motivation, opportunity and rationalisation (Johnstone and Wong, 2008). Others state

personal characteristics of the perpetrator, motivation and opportunity (Sampson, 1999 , KPMG, 2007). Motivation for fraud refers to the situation that drive people to commit it. These could be economic or even peer pressure. Opportunity on the other hand is the condition that allows the fraudster to create a deception to commit fraud. Lax control systems for instance can give opportunity to fraudster to create deception to execute their intentions of fraud. Rationalisation refers to the behaviour of fraudsters to rationalise the act by convincing themselves that committing fraud is okay.

Personal characteristics refer to the character of an individual that gives them the inclination to commit fraud. Cultural and personal values determine what people consider to be important and beneficial and these determine the standards and behaviour of people. Hence values certainly plays a part in the personal character of a person that could make him inclined to commit fraud or not. Cultural and Personal values should therefore be taken into consideration when the protections of systems are being designed.

Though various programs can be implemented to dissuade fraudsters from committing fraud the only condition that could be controlled by targeting business processes is opportunity. This should be such that the mechanisms that enable deception is removed.

2.6 Summary

In summary rural banking regulation create small banks that need other organisations that could be susceptible to fraud. They also operate in a unique environment that could enhance or inhibit fraud control capability. To add to that they have a paradoxical situation where they are regulated by an organisation they own. On the other hand rural

banks as community banks use intimate business methods to understand their environment well and this could be an asset in fraud control.

After discussing the issue of fraud the conclusion is that it is primarily a theft which is enabled by deception. Understanding the methods used to create the deception can be a useful means to dealing with it. Analysing notable fraud cases show four main types of deception.

With the profile of a fraudster fitting so many people targeting certain people in fraud prevention cannot be effective. However it was also shown that among the conditions which enable fraud opportunity to commit fraud is the one that can be controlled most by an organisation and this should be the focus of fraud prevention programs. The next chapter discusses the approach to dealing with fraud risks.

Chapter 3

3 Dealing with Fraud

This chapter explores the issues that have to be taken into consideration in controlling fraud. It starts with the analysis of the issue of managing risks and then discusses internal control as the primary means of dealing with fraud focusing on information security as a key tool. It further discusses translating and aligning internal control goals and information security goals and to the goals of all stakeholders. A discussion of conventional fraud and banking controls is also done. Finally a discussion of various fraud and banking controls are currently in use is done.

3.1 Managing Risks

Having analysed the nature of fraud risks the question is how to deal with it. The task of managing risk involves two main activities namely risk analysis and risk management (Gerba and Solms, 2005).

Whiles risk analysis involves the process by which an organisation identifies, estimates (in terms of probability of occurrence and the level of damage) and finally evaluates risk (level tolerance of the organisation). Risk management on the other hand refers to

the process of planning, monitoring and controlling activities based on the information produced by the process of risk analysis. Risk management explores the possibility of risk avoidance, risk transfer, risk acceptance or risk mitigation (Hillson, 1999). In dealing with banking risks, there are different approaches depending on the type of risks. The main aim of this research is to identify mitigation mechanisms.

In the case of managing market or credit risks the key is in acquiring the knowledge and understanding of these risks and applying this knowledge transaction by transaction. Parameters like credit rating and expected default rate are used to measure credit risk of specific borrowers. These methods assess the risks associated with each transaction and the parameters used form the basis for deciding how to handle the risk associated with each transaction.

Managing operational risk on the other hand cuts across various functions in the organisation and may exist in marketing and credit risk areas (Shabudin, 2007). The 2008 credit crunch that affected banking systems around the world had its roots in the failure to manage credit risk properly and hence engaging in subprime lending (Wallace et al., 2008) however the main cause of this is the failure of risk management and regulatory processes to identify the credit risk. It was in essence an operational risk failure. In managing operational risk it is very important to have a holistic view of the organisation.

Loss data does not seem to be a very effective means of predicting operational risk incidents as is the case for other forms of risks (Thirlwell, 2002). This is partly because when organisations are hit by incidents, controls are changed immediately and also because empirical evidence is a poor guide to predicting rare events like operational risks. Also in the particular case of fraud the adversary is intelligent and is trying to

create a deception and so would seek avenues to do just that. In dealing with these type of threats, it is most effective when one does not make arbitrary assumptions about the threat (Schneier, 2005b). The argument is that with a large number of potential risks it is irrational to focus on individual targets as a means of mitigating potential attacks. A more proactive systemic approach seems to be the best means to deal with operational risks and fraud. This approach stands a better chance at covering it in all of its manifestation. It also has a better chance to identify the risk before it is causes a loss.

There are various recommendations for dealing with operational risks. The Risk Management Association recommends that a good operational risk management framework must have four basic elements namely leadership, management, risk, and tools (Taylor, 2006). Leadership determines the right culture and environment with management being a set of processes that channel and control the institution's risks. Risk element of the framework involves understanding the pattern of operational risks the organisation faces and takes on whereas tools refer to the collection of guides, templates, libraries, services, training, and software that are available to fight the risks. A similar framework for dealing with operational risk also has four element these are strategy, process, infrastructure, and environment (Haubenstock, 2001).

There is an increased awareness to develop operational risk management models looking up to international and national regulation and standards for guidance (Crawford and Hoppe, 2005). Each organisation or industry is however different whereas standards like the COSO framework and models are always generic (Crawford and Hoppe, 2005). According to the well known McKenzie's 7 s' model developed by Tom Peters and Robert Waterman, two consultants working at the McKinsey & Company consulting firm, there are seven internal aspects to consider in the analysis of

an organisation. The general premise is that for companies to be effective there must be a fit between these seven elements. This should be the start to customising standards and generic models. The McKenzie seven S's comprise of three hard elements and four soft elements. The hard elements are strategy structure and systems whilst the soft elements are shared values, skills, style (management) and staff. This means that a workable model for one institution could be very unsuitable for another similar organisation sometimes in the same industry. Hence there is the need to find suitable operational risk management model for every organisation especially for a complex business environment as is the case in the Rural Banking system in Ghana. In designing systems to deal with risks it is important to transform the needs of the systems context into the requirements for the new system and to redesign the application context around the new system to better exploit its capabilities and avoid negative reactions from users (Donzelli and Bresciani, 2004). There is also an emerging view that quantitative processes for managing risks are adequately known and applied however failures and problems arise more because of the softer issues (Turnbull, 2004). These soft issues within an organisation relates to issues such as politics and people's feelings, leadership, organisational culture, readiness for IT upgrades, behavioural style, job involvement, commitment, fairness, motivation and job satisfaction among others.

3.2 Internal Control

Good internal control reduces operational risk and fraud (General Accounting Office, 2002). Internal controls can be used to better manage the way in which employees, partners and customers and how their access to corporate resources is controlled and audited to mitigate some of these operational risks (Small, 2004). They are therefore put in place to keep companies on course to avoid unforeseen events, reduce risks of

asset loss, promote efficiency and help ensure the compliance with laws and regulations (Committee of Sponsoring Organisations of the Treadway Commision, 1994). Internal controls are necessary because of mental, moral and physical weakness inherent in people who run business systems (Bower and Schlosser, 1965) (Calbom, 2002). They are therefore needed to make a system more reliable and reduce the opportunity for people to make errors or to perpetrate various types of fraud and other improper actions. They are mostly aimed at controlling the unreliability of people; a situation that leads to errors and fraud. It is therefore important that internal controls are not left to the discretion of people which it aims to control.

Internal control has been described as the systems, policies, procedures and processes effected by the Board of Directors, Management and other personnel to safeguard banks assets, Limit or control risks and achieve a banks objective (Comptroller of the Currency Administrator of National Banks, 2001). The board of directors of an organisation determine business strategy, and determine all major goals of an organisation. This could therefore be used to ensure that internal control is totally in line with business goals and aimed at achieving such goals. Though internal control processes and procedures operate at the lower level of the organisation, it is important for the board to set the tone and create a culture of internal control within an organisation.

Another definition of internal control has referred to it as the mechanisms used by organisational leaders to convey strategy, vision and desires to the rest of the organisation (Pathak, 2005). This further point to the fact that internal control must be in line and be used as a means to achieving organisational goals and supports the position that internal controls are very important to the achievement of compliance in

organisations. According to Pathak (2005) internal controls is manifest in the form of standards, policies, procedures and rules and that proper internal control allows the organisation's risk management support to work effectively and in harmony. Internal control works at all levels of the organisation. Control policies and procedures must therefore be designed into every system in the organisation rather than as separate superficial rules that sit on a potentially insecure system that has been designed without control considerations.

Whiles it is recognised that internal control is the responsibility of all the people in the organisation, the identifiable groups within the organisation mentioned in the COSO framework are management, board of directors, internal auditors and other personnel. What is clearly not mentioned is the role of information systems personnel. For most modern organisations, business processes are run by computer systems where computers modifying data in databases form the core of transactions. The implementation of any internal control system should in effect be the control of the use of these computer systems. Obviously the mechanism which can be used in controlling these systems is information systems security.

The United States General Accounting Office (GAO) and the Bank for International Settlement's Basel Committee both consider the following as the elements of internal control;

1. Management oversight and the control culture (Board of directors, Senior management, Control culture)
2. Risk recognition and assessment,
3. Control activities and segregation of duties,
4. Information and communication,

5. Monitoring activities and correcting deficiencies (Basel Committee on Banking Supervision, 1998 , General Accounting Office, 1999).

Though internal control means different things to different people it is generally seen as a process and that its effectiveness is measured at any point in time by the condition of any of the five components mentioned above.

3.2.1 Control Environment

There have been different descriptions of the environment relevant to internal control. The Committee of Sponsoring Organisation of the Treadway Commission indicated that the control environment generally sets the tone of the organisation influencing the control consciousness of the people (COSO, 2005). It is the culture that encourages the implementation of control measures in it. The GAO (1999) refers to ethical behaviour, guidance for ethical behaviour, removal of temptation for such behaviour, discipline and the need to competence and provision of the right skill for people doing specific jobs. There is the need to create the culture within the organisation such that its members are security conscious. All these are achieved through the leadership style of management.

The control environment however has been referred to by some authorities as the internal environment and described as the people within the organisation and the organisational culture (Committee of Sponsoring Organisations of the Treadway Commision, 1994 , General Accounting Office, 2002). Whilst there is no doubt that the internal environment is very important to the success of the internal control function it neglects a very important factor which is the external environment. No organisation is an island hence systems and their external environment are intertwined so need to be treated and analysed as a larger socio-technical system. This is to ensure that their

overall needs can be understood in order that the most appropriate socio–technical requirements can be identified (Offen, 2002 , Donzelli and Bresciani, 2004). The Risk Management Association however defines the business environment with regards to internal control measures as the internal and external circumstances of a firm's businesses that can materially affect its operational risk profile (The Advanced Measurement Approached Group, 2008). This definition seems more appropriate given the emphasis on both the internal and external environment. Marketing and business strategy experts have long sought to understand the environment they operate in as a means of increasing likelihood of the organisation achieving their objectives. The idea is that various factors within and outside the organisation can present opportunities or threats to its goals. Though these experts cannot influence most of the elements of external environmental factors they study it to take advantage of it. This is because they are well aware of the advantages of using these characteristics to their advantage. In the same way risk managers and information security specialists could start using an external environmental scan as a means of identifying the opportunities whilst identifying the threats.

In the rural banking system, the control environment should be expanded to take into account the socio cultural character of the industry to be able to ensure better protection of the banking system.

3.2.2 Risk Assessment

The second element of internal control involves a risk assessment. The Basel Committee recommends that risks that could adversely affect the achievement of a bank's goals be identified and continuously assessed (Basel Committee on Banking Supervision, 1998). Whilst it is of utmost importance to determine the risks that an

organisation faces in order to determine controls, the methods for deriving what risks are to be taken into account makes a lot of difference. Risk assessment is said to generally involve a process by which an organisation identifies, estimates and finally evaluates risks to achieving objectives (KPMG, 1999). It is therefore the process of analysing and interpreting risk as a basis for determining how they should be managed. Risk assessment must look at all relevant interactions between various objects or subjects and their impact on the risk events. The Basel committee indicates that an effective risk assessment identifies and considers all internal and external factors that could adversely affect an organisation's performance (Basel Committee on Banking Supervision, 1998). Some of the issues that should be considered are the complexity and effects of the organisation's structure, the type of the business activity and business processes, the quality of personnel, organisational changes and employee turnover. External factors like fluctuating economic conditions, changes in the industry and technological advances must also be considered.

The national institute of standards and technology proposes a nine step process to conducting an IT risk analysis (Stoneburner et al., 2002). These are system characterisation, vulnerability identification, Control analysis likelihood determination impact analysis risk determination control recommendation and result documentation. Others also propose a process involving system characterisation, threat identification, vulnerability identification, risk analysis, control recommendations and results documentation (Bowen et al., 2006).

System characterisation establishes the scope of the risk assessment effort, delineates the operational authorisation boundaries, and provides information whilst the threat identification undertakes a comprehensive identification of threat sources with the

potential to exploit weaknesses in the system. Vulnerability assessment identifies all vulnerabilities which are flaws or weakness in system security procedures, design, implementation, or internal controls that could be exercised accidentally triggered or intentionally exploited and could result in a security breach or a violation of the system's security policy.

Next is risk determination or estimation of risk to the system. This analysis primarily aims at reducing the range of vulnerabilities to the ones that matter. Whilst this is desirable it could have a potential of being counterproductive. This is primarily due to the methods currently used to achieve this.

Risk determination aims to consider closely intertwined factors, such as the security controls in place for the system under review, the likelihood that those controls will be either inadequate or ineffective protection for the system and finally the impact of that failure. These activities involve control analysis, likelihood determination, impact analysis and risk determination. Generally risk is determined as a product of the impact or the impact/value (V) of loss with the occurrence of the risk and its likelihood/probability (P) of the occurrence of the risk.

$$Risk = P \times V$$

When this value is computed for a single event it is called single loss expectancy (SLO). Multiplied by the annualised rate of expectancy (ARO) a value referred to as the annual loss expectancy (ALE) is obtained.

$$ALE = SLO \times ARO$$

The annual expectancy model (ALE) seeks to estimate the value of risk as a means to decide whether possible losses are such that mitigation measures need to be taken. It also seeks to use that as a basis to prevent the cost of mitigation from exceeding the possible loss. It is therefore used as a measure of the cost of effective security (Anderson et al., 1994).

Another popular model involves the use of a risk matrix. See figure 3.1. This involves assessing the likelihood and impact of risk events as high, medium or low. Risk events are classified as Risk Scale: High if the value is between 50 and 100); Medium if between 10 and 50; Low if between 1 and 10.

		Impact		
		Low (10)	Medium (50)	High (100)
Likelihood	High (1.0)	Low 1.0x10=10	Medium 1.0x50=50	High 1.0x100=100
	Medium (0.5)	Low 0.5x10=5	Medium 0.5x50=25	Medium 0.5x100=50
	Low (0.1)	Low 0.1x10=1	Low 0.1x50=5	Low 0.1x100=10

Figure 3.1 Risk Matrix (Stoneburner et al., 2002)

Both methods of assessing risk require that risk events must be identified and their probability of occurrence estimated. This can however be a difficult thing to do especially in operational risk estimates where occurrences of risk event are rare and varied.

The problem with both models is therefore the inability to accurately estimate the probability and the value of the corporate resources that would be at risk if the loss event occurs. An assigned probability depends on the information available to the

analyst at the time of the analysis. At best, probability measures perceived risks and even when it does its usefulness is limited because of its level of subjectivity in the absence of an objective means of measurements (Holton, 2004).

Now even when objective probabilities are known the issue of whether the loss event grabs ones attention comes to being. This depends on the perceived level of potential damage that could arise commonly referred to as exposure or the impact. Usually the final exposure that is settled on depends on what the preferences of the analyst are and what information is available (Arrow, 1964). This also indicates that you most often than not end up with a perceived exposure.

Holton (2004) has indicated that risk is a human condition where self awareness is key. In other words there is no risk in the absence of self awareness. This implicitly raises the question of using risk determination as the basis of managing adverse events that could befall an organisation especially when information on the level of uncertainty and exposure is scanty.

Generally risk is relative and in certain cases intuitive (Holton, 2004). The likelihood of an adverse event occurring is different from bank to bank. On the other hand there could be as many exposures as there are propositions. The bottom line here is that there are many variables in rural banking and depending on the size and other operational factors certain risks could be more serious than others. In that regard, effective controls and protection mechanisms for the rural banking system must be designed based on the entire range of existing vulnerabilities. This would leaving implementation within individual rural banks to individual risks manager based on the condition of the bank at any particular time. This will also allows the system to have an element of human

configuration and also enables it to be shaped to suit the nature of the each organisation.

3.2.3 Control Activities

Control activities are supposed to occur at all levels and functions of an organisation it involves. Control activities include top level and performance reviews, compliance with exposure limits, approvals, authorisations Verifications and reconciliations physical and activity controls (Basel Committee, 1998). Other activities include reconciliation, and the creation and maintenance of related records which provide evidence of execution (KPMG, 1999). Others propose seven basic kinds of internal control duties (Bower and Schlosser, 1965). They are supervision, clerical proof, acknowledging performance, transferring responsibility, protective measures, review and finally verification and evaluation. On the surface these controls could be implemented in all organisations in any part of the world. This might however not be the case see Chapter 4.

Banking regulatory regimes most often do not introduce or enforce control mechanisms that reduce operational risks. This is because supervisors and regulators concentrate on prudential regulation aimed at protecting depositors and the banking system as a whole. Regulators use mechanisms like reserve requirement, capital adequacy ratio etc to achieve this. The Basel Committee recommends that a portion of a banks working capital be set aside to cover operational risks (Basel Committee on Banking Supervision, 2001). Though it is desirable to have these measures in place to deal with adverse events when they occur, it is always desirable to prevent it from occurring in the first place and they do not so that. Reserve requirements can however be an incentive to compel bankers to put in place internal control measures usually referred to

as non-prudential regulation. Aside the benefits of reduced risks, there are other collateral benefits of good internal control. This is because the quantum of a bank's reserve requirement depends on the level of operational risks it is exposed to. A reduction of risks could therefore lead to a reduction in reserve requirements.

Information security is becoming important in implementing controls. This is because when organisations are computerised and linked together, they exchange information and engage in transactions in ways unanticipated before. The importance of information becomes core to most business activities without which business will fail to operate (Owen, 1998). With this in mind, the security of information could become the key to securing corporate assets. With the increasing use of information systems in operations, internal controls need to be supported by a system that is in step with the nature of the risks. Information security also becomes important to ensure enforcing adherence to controls. A good information security system which is set up to deal with the risks is the best way to deal with the current nature of threats.

The paradigm being discussed here is the use of information security techniques as a tool for reducing operational risks. Traditionally information security has been concerned with securing information within information systems and not as a tool to reduce the overall risk of the organisation. This paradigm is captured in the statement

> *"failures of information security are clearly adverse events which cause losses to business; therefore information security is a risk management discipline"* (Blakley et al., 2001).

No doubt that the introduction of information systems exposes business to new kinds of risks and the immediate focus is to put measures in place to deal with such risks. It is

however time for information security to be transformed totally from a self serving objective that focuses on the unique risks emerging from the use of information technology to looking at the opportunities of employing some of these techniques for general business risks reduction.

With concepts like electronic money etc it is clear that information resources increasingly represent the resources of an organisation. There is the need to protect these resources and information security is the best means to do that because it is the means for controlling the activities of users within an information system. The preference of the use of these techniques in implementing control measures is because it can automate the prevention mechanisms and force employees to comply with internal control procedures.

Granting access without understanding risks cannot prevent fraud. This position becomes more critical where operatives who have authorised access to these resources could misuses their genuine authority to defraud the organisation (Foundation of Research and Education, 2005). Risks should therefore be thoroughly understood before access controls are designed. It calls for information security specialists to look beyond issues like authorised access to look at issues relating to whether the information being accessed is used properly. In essence looking at either technology and risk management in isolation can be flawed, the two disciplines are intrinsically interlinked and the field of security tends to be the meeting point (Wilson, 2005).

Information security, we must understand, is not a panacea to operational risk and internal control. However it can be an excellent operational risk reduction tool if it is deployed properly taking into consideration the environment in which it is going to operate and supported by appropriate policies to enforce the technical controls

(Anderson et al., 1994). As always with technological products, the behaviour of users goes a long way to determine its effectiveness. Assuming if the front door to your house is protected by the most reliable door lock and you do not care to engage the lock on your back door the security of your house is as good as nothing. People should always be considered in designing protection mechanisms.

3.2.4 Information and Communication

To make an internal control system effective, pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information such as operational, financial and compliance related reports that help the control of the business must be disseminated. It is very important that all the members of an organisation are made aware of the laws, policies and procedures. Employees are also given information to help them understand their role in relation to others in the organisation. In addition reports on performance need to be sent across to users to awaken them to their control responsibilities.

When disseminating information the content, timeliness, accuracy, accessibility and how up to date the information is must be taken into consideration (Committee of Sponsoring Organisations of the Treadway Commision, 1994).

3.2.5 Monitoring

Internal control systems need to be monitored to ensure that internal control continues to operate effectively. This is a process that assesses the quality of the system's performance over time (Committee of Sponsoring Organisations of the Treadway Commision, 1994). A good internal control environment requires that there is a clear organisational structure and clearly defined areas of authority and responsibility and appropriate lines of reporting. Ongoing monitoring occurs during the course of

operations or as separate evaluations which depend on the level of ongoing monitoring. A combination of ongoing and separate evaluation processes is also possible when it comes to reporting on deficiencies and these reports must be directed upstream.

3.3 Information Technology Compliance and Business Controls

It is important that the goals of a fraud control system are aligned with the goals of all stakeholders in an organisation. In the case of the rural banking industry it is important to align the goals of a fraud protection system to all stakeholders and these would include shareholders, communities, management and regulators. Security systems have multiple players and each player has an agenda which might not necessarily be in line with other players (Schneier, 2006). In that regards, for mechanisms aimed at achieving the security objective to succeed, the player made responsible for enforcing it must be in line with the player's vested interest.

Many frameworks support the alignment of security goals to corporate goals (Swanson and Guttman, 1996 , Information Technology Governance Institute, 2005). Unfortunately, security is sometimes viewed as thwarting the mission of the organisation by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. Security rules and procedures however do not exist for their own sake. They are put in place to protect important assets and support the overall organisational mission and they are a means to an end and not an end in itself (Swanson and Guttman, 1996). IT governance aims to match corporate goals and information technology goals and to ensure that information systems promote corporate goals and takes the responsibility of this function from the IT department and gives it to the board of directors. It is however desirable not only to align the goals of security and control

systems to corporate goals but to the goals of all other stakeholders to ensure its success.

3.4 Threat Identification, Security Requirements and Specification

Security goals usually referred to as security requirements are optative descriptions of what the system is to do (Haley et al., 2004). Security requirements do not describe how security is to be implemented but instead describe what is desired. Generally internal control objectives arrived at in a risk management exercise should be the basis of the security requirement. The identification of security requirements must therefore be looked at from the point of view of what is required to make the system secure and not the specific solution to be implemented.

In identifying vulnerabilities and threats, reasonable trust assumption should be made and that would require that we trust the properties of some domains and to go no further in the analysis (Haley et al., 2002). This means that we would have a belief that the domain would participate competently and honestly in the satisfaction of the security requirement. However there must be a basis to arrive at such a trust assumption.

In analysing security vulnerabilities and threats it is important that all the parameters of domains outside a trust assumption are optative hence one would have to question all the properties and operations of objects to confirm them as objectively true (Haley et al., 2006). In deriving the security goals of a fraud control system for the rural banking system, the concern would be whether the information being passed on to the next subject (whether a person or the computer system) is objectively true. For instance when a cheque is presented to withdraw cash an issue would be whether we can

reliably confirm that the account holder wrote and issued the cheque. This should form the basis of identifying vulnerabilities and threats to the system and designing solutions to deal with the threats.

Security specifications is the description of the behaviour of the domain in terms its phenomenon indicative or optative visible at its interface (Haley et al., 2004). In other words security specification looks at how the security requirements are to be achieved through specific externally visible characteristics. They are therefore technically inclined. Control activities come under security specification these are the mechanisms that are to be implemented to deal with the threats identified and described in a risk assessment. A fraud control system would therefore focus on what external visible characteristics would be of interest and how they can indicate that there is not fraud.

3.5 Information Security

With a clear specification of what a security systems is to achieve there is a toolbox of security mechanisms and models to help in operational risk management and fraud control. Information security has been defined as *"the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities*" (British Standards Institution, 2005). Information security principles cover various inherent elements of an information security system. The primary elements of information security are widely accepted as confidentiality, integrity and availability, commonly known as the CIA triad (Stewart et al., 2005). Though these are considered the core aspects of security other elements have been presented by various researchers. One of such models presented the six elements of security namely availability, utility, integrity, authenticity, confidentiality and possession (Bosworth and Kabay, 2002).

The CIA triad has been classified under two characteristics. These are protection or fault introduction and behaviour in terms of the output (Jonsson, 1998). Protection involves influence of the environmental on the system whiles behavioural is concerned with the behaviour of the system that are manifest. The emphasis on any particular element of security depends on what security means to the user. Whiles military systems emphases confidentiality commercial systems emphasised integrity (Clark and Wilson, 1987).

To develop an information security system it is important to start with a security policy which describes the information security needs of an organisation (Anderson et al., 2001). Security policies are only statements describing the security objectives of an organisation that must be enforced. To enforce these policies a combination of procedural and technical measures are used. These measures designed to deal with information security risks fall into 4 main groups (Blakley et al., 2001). These are namely:

- Protection measures that prevent adverse events from occurring
- Detection measures to discover unauthorised activities
- Response measures to deal with adverse events when they occur and to return the system to a safe condition.
- Assurance measures to validate the effectiveness of the protection, detection and response measures

3.5.1 Confidentiality

Confidentiality refers to the security property that concern controlling unauthorised access, disclosure and use of information in an information system whether it is stored, in transit, being processed. The security objective of confidentiality is the element of

information security that preserves authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (McCallister et al., 2009). Organisations require confidentiality to prevent critical information from getting into the hands of criminals who could use the information to perpetrate fraud or attack the organisation or its stakeholders in some way. These could lead to loss of resource or reputational loss.

Organisations particularly desire to keep personal identification information confidential in a bid to prevent impersonation. Achieving confidentiality is therefore sometimes necessary to achieve other security requirements of organisations like integrity. This can be seen in a case where passwords have to be kept confidential to prevent unauthorised access which can lead to breaching integrity requirements. Achieving confidentiality however would not be a primary focus of this research.

3.5.2 Integrity

Integrity on the other hand deals with controlling how information resources in an information system are changed or used. It has been described as an element of security guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity (Barker, 2003). Achieving this objective is important to prevent fraud.

Integrity is examined in three perspectives (Stewart et al., 2005)

1. Unauthorised subjects should be prevented from making modifications
2. Authorised subjects should only make intentional modifications and must be prevented from making unauthorised modifications that as a result of error or fraud

3. Objects should be internally and externally consistent so that their data is correct and a true reflection of the real world and any relationship with a child, peer and parent object is consistent and verifiable. This is the main requirement that is breached in the bid to create deception in the process of committing fraud.

3.5.3 Availability

Availability on the other hand looks at providing prompt access to the information stored on the system. Availability ensures timely and reliable access to and the use of information (National Institute of Standards and Technology, 2004). Availability is not a key objective in preventing fraud.

Aside the three main elements of information security in the form of the CIA triad there are other security attributes that are also very important. These include accountability and non repudiation.

3.6 Accountability and Non Repudiation

Accountability is the property that gives the security system the ability to track who has had access to or changed information resources. It is important to ensure that every user is the one who actually performed an activity being attributed to them. This brings in the issue of non repudiation which is the security objective that seeks to prevent users from denying previous commitments or actions performed within the system (Menezes et al., 2001). Mechanisms used in a security system must be such that there is little room for doubt what subject has performed a particular transaction.

Non repudiation is usually achieved using digital certificates and digital signatures. The idea is to mark an identity with a public encryption key such that a transaction can only

be traced back to the subject bearing that identity without the possibility of denial. This is discussed shortly.

3.7 Authorisation and Access Control

Authorisation is the right to undertake certain actions within an information system. This naturally follows authentication of an identity. In other words when a subject is verified to be who they say they are then the issue of what they are allowed to do comes in. Authorisation is usually determined within access control policies and models. Most authorisation models are based on traditional three-way concepts of a subject object and access type (Jøsang et al., 2006). The relationship is such that the subject requests access to an object which is a resource. Access type refers to the type of access granted to the subject for an object. This three way relationship is determined by the owner/custodian of the object/resource. The objective of access control is to manage this relationship (Anderson, 2001). There are two main types of access control concepts; mandatory access controls and discretionary access controls. To prevent fraud, access control would exactly be the framework within which the control of relationships between customer and employees and various banking objects would be done.

3.8 Mandatory and Discretionary Access Controls

The formal definition of mandatory access control (MAC) describes it as information flow restrictions enforced independent of user actions as opposed to the discretionary access control (DAC) where the user has the ability to change security attributes of the object. It is generally accepted that discretionary access control is not a desirable policy for managing systems (Farraiolo and Kuhn, 1992 , Anderson et al., 2001) because

organisations information do not belong to individual users. It is therefore inappropriate to leave security management of these resources to individual users. Also DAC cannot ensure the implementation of a unified security policy because access to resources is at the discretion of users and not enforced centrally like MAC (Anderson et al., 2001). To use an access control model to enforce fraud controls, it will require enforceable mechanism as they exist in MAC because discretionary form of access control can undermine an organisation's fraud control policies.

3.9 Multilevel and Multilateral Security

Multilevel security models classify security properties into various levels some higher than others. Data objects are assigned a security label. Models then determine which security levels can be accessed by which subjects and the rules about the type of access. There are other security models that have been designed based on other principles other than a vertical graduated scale of security labels. There is sometimes the need to compartmentalise information with the same security label to prevent lateral flow making different compartments available to different subject with the same security label or classification. It is usually assumed that subjects with the same security level would have the same access to information but in certain cases there is the need to regulate such information access. Multilateral security is necessary especially when there is a conflict of interest situation. Models like the Brewer-Nash's Chinese wall security model to be discussed shortly deals with such situations.

Though it is argued that multilevel security policies cannot deal with commercial security concerns (Clark and Wilson, 1987), lattice based security designs are shown to deal with some considerations depending on what attribute is most desired (Sandhu, 1992 , Sandhu, 1993). The inference of this is that different models fit different

contexts and there is the need to craft a security model to enforce the fine details every context requires.

3.10 Information Security Policy

A security policy is a succinct statement of the protection properties that a system, or generic type of system, must have. In other words a security polices expresses clearly and concisely what a systems protection mechanisms are to achieve.

With a clear statement of what these objectives are, security models are constructed as an abstract presentation of how these security goals are to be achieved and are designed to implement the security policies of an organisation. The general pattern that most security policies follow is that a subset of the states of the system as secure is first defined (Anderson et al., 2001). Transition rules that guarantee that objects remain in a secure state when they move from one secure state to another are then defined and this is the basis of preserving the security of the system. These models are generic and value neutral. They are also not constrained by the technological considerations needed to implement them.

3.11 Bell-LaPadula Security Policy and Security Properties

Confidentiality was the prime motivation in the military for security is characteristic that drove the early security models (Sandhu, 1993). The Bell-LaPadula model was the first such security model to appear to address the issue. It met security requirements by classifying data and information into confidentiality classes based on the sensitivity of the information whiles users were allowed to access these classified information based on their level of security clearance/category. It introduces many principles to support classification and user clearances. These principles are useful in many of the models

that have followed. The Bell–LaPadula model makes use of various properties like the high or low tranquillity property which looks at changing security properties during system operation (McLean, 1982). This is linked to high water mark property which requires every subject, no matter the security label, to start each session with the least privilege and be upgraded when an object with a higher security label is accessed (Anderson et al., 2001). This is to avoid disclosure problems. This however could arise in over classification where the gradual upgrade of a subject's security label results in it writing only high label objects. It could become a problem when an application which has been upgraded cannot see lower files to continue work when it has been upgraded.

Other properties like non-interference (Goguen and Meseguer, 1982) and non-deducibility (Sutherland, 1986) were introduced to control what users can see and what they can do with the information they see. In non-interference actions by higher subjects does not affect what a lower subject can see whilst in non deducibility lower subjects can see but cannot understand or make deductions from actions of higher subjects.

Some difficulties were also brought to light and these include composability, covert channels, polyinstantiation and aggregation. A security property is composable if it remains intact even when it runs alongside other security mechanisms in the same system (Canetti, 2008). It looks at the issue of different secure systems becoming insecure when connected together. Covert channels refer to situations where backdoor channels allow the flow of information from a high security label to a low security labels. Polyinstantiation on the other hand occur when an effort to have different versions of data for different security labels ends up with inconsistent data.

3.12 Brewer-Nash Model (Chinese wall Security policy)

The Brewer-Nash policy is a multilateral security policy in that it deals with the disclosure of information hence focus on confidentiality. The Chinese wall security policy (CWSP) is a mandatory access control policy. It however has a voluntary element to it in where users can choose which information they would like to see implicitly denying themselves the right to information from conflicting classes. It was a specific design with the financial industry in mind. Financial institutions providing corporate business services to other organisations can have insider knowledge of its rivals making and the disclosure of such information is highly unethical and could lead to legal action. When an analyst in the firm has information on a client they must be denied information of rival firms in order to prevent unauthorised disclosure. In other words such an analyst must uphold the confidentiality of information provided to him by his firm's clients and not advise organisations where he has insider knowledge of the plans, status or standing of a competitor. The CWSP operates at three levels.

1. At the lowest level individual objects containing specific data items are considered, each concerning a specific company.
2. At the intermediate level all objects concerning the same company are grouped together. These are referred to as ‘company data sets’.
3. At the highest level all company data sets whose corporations are in competition or conflict, are grouped together. They are referred to as conflict of interest classes (Brewer and Nash, 1989).

The main rule in the CWSP is that once a subject has accessed an object the only other objects accessible by that subject can come from the same company dataset or from a different conflict of interest class (Minsky and Ungureanu, 1998). In other words an analyst can get information about any company but once the analyst gets information

about a given company, they are not allowed to get information about any other company in the same conflict of interest class. This means that a subject can at most have access to one company dataset in each conflict of interest class and any information that an analyst can get from a system depends on what they have accessed in the past.

The problem with this model is that it assumes that conflict of interest is static. This is not so especially when the interest of companies constantly change and may have different types and levels of interest in other companies. Conflict of interest(CIF) classes can therefore overlap, and the assertion of having completely disjoint conflict of interest classes is challenged in the variant known as the Aggressive Chinese Wall Security Model (ACWSP) (Lin, 1989). In the CWSP conflict of interest are mutually disjoint sets however the ACWSP conflict of interest classes can overlap. The scenario used was that if an airline company A has an interest in company B and a petroleum company C also has an interest in company B they could be considered as being in the same CIF. In the CWSP such a conflict cannot exist were CIF classes are disjoint and this is one problem the ACWSP resolved.

The access control model for data mining environments, a model based on the Chinese wall policy, draws from the aggressive Chinese wall security policy and makes use of overlaps in conflicts of interest data classes to ensure data integrity. It however identifies two other problems that were thought to be outstanding (Loock and Eloff, 2005). The first is that the severity of the conflict between two companies should be definable. This is because the level of conflict may be such that it is negligible and may not affect access to information. The other issue was that the security policy model should be dynamic. That is to say situations change and if a company acquires an interest in another company it might come into conflict with other companies that it

previously was not in conflict with. On the other hand if a company ceases having an interest in a company that it previously had an interest in, it also ceases to be in conflict with companies that it was in conflict with. Loock and Eloff (2005) propose two mechanisms to dealing with these problems. The first is to define a conflict of interest sphere around a company and this is defined by a radius **r**. The second is to define the severity between two companies which is defined as the distance. On one hand when the radius is higher, the more interests a company has and potentially more companies it could be in conflict with. On the other hand the higher the distance between two companies the lower the conflict between them.

The CWSP and its derivative models looks at the historic activity of a user and assigns the users rights to other data objects. Applied to transactions, a user's historic activity on a system could be used as means of preventing fraudsters from executing two unrelated transactions to enable fraud. The introduction of concepts like the sphere of conflict and the extent of the conflict could be used to determine the extent to which transactions performed by employees in the past conflict with current transactions.

3.13 Biba Integrity Model

The Biba integrity Model was the first security Policy to focus on integrity issues (Anderson et al., 2001). The Biba model recommends that no information can be written from a lower security/impure level to a higher/pure security level in direct contrast to Bell-LaPadula. Whilst Bell-LaPadula can allow a higher security level to read from a lower level Biba cannot allow a higher security level to read from a low level for the fear of the lower level contaminating the higher level. On the other hand the lower security level is not allowed to write to a higher level for the same fear of

contamination but BLP would rather not allow a higher security level to write to a lower level for the fear of leaking confidential information.

A key principle introduced by the two models is the tranquillity principle which looks at the issue of changing the security label of a subject and object based on what it has accessed or has accessed it respectively. This can be linked to the mechanisms of the Chinese wall policy where a change to the level of conflict is made when circumstances regarding a subject's activities regarding an object changes.

3.14 Clark – Wilson Model

The Clark – Wilson Model was inspired by the double entry bookkeeping system (Anderson et al., 2001) to maintain integrity in commercial transactions. Double entry bookkeeping is a primitive accounting practice that requires that a transaction is entered into two accounting books one as a credit and the other as a debit. At the end of the day all the accounts add up and balance out to zero. With most organisations having different clerks in charge of different books it requires more than one clerk to commit a fraud.

The Clark – Wilson model identifies two important mechanisms that are at the heart of control of fraud in commercial organisations. These are a well formed transaction and separation of duty (Clark and Wilson, 1987).

3.14.1 Well formed transaction

A well formed transaction is generally an operation on a data item. The concept of the well-formed transaction is that a user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data. A well formed

transaction is also referred to as a Transformation Procedure (TP). It recognises the importance of the mechanisms of a business process in the maintenance of integrity.

3.14.2 Separation of Duty

The principle of separation of duty involves the practice of dividing and allocating different tasks in a business process to different individuals to prevent a single individual from misusing the process (Hu et al., 2006). Perhaps the most basic separation of duty rule is that any person permitted to create or certify a well-formed transaction may not be permitted to execute it. This rule ensures that a minimum of two people are required to cause a change in a well formed transaction. The rationale for separating duties is to discourage fraud. By distributing the responsibility and authority for a task over a number of people it raises the risk by introducing the mandatory involvement of more than one individual in a fraud (Simon and Zurko, 1997).

The basis for dividing a business process into tasks for the purpose of implementing a separation of duty policy is the existence of a conflict (Perelson, 2001). Conflicts are said to arise when the execution of two tasks by a person creates a vulnerability which exploited could threaten the business and its goals or lead to the loss of some resources. Table 3.1 showing the various levels of conflict that can arise.

Conflict	Static	Dynamic
Conflicting Roles	May not have the same user or conflicting users as members	May not be assumed by the same user (or conflicting users) in one process instance
Conflicting Permissions	Must be assigned to conflicting Roles	May not be exercised by the same user (or conflicting users) for a specific process instance
Conflicting Users	May not belong to conflicting roles	May not perform conflicting tasks in the same process instance
Conflicting Tasks	Must be assigned to conflicting roles	May not be executed by the same user (or conflicting users) in the same process instance

Table 3.1; Conflict of entities paradigm (Perelson et al., 2001)

In defining separation of duties the focus has always been either on the user, the role or on the permission with one factor being the focus at any one time. So there can be situation with conflicting users, conflicting roles or conflicting permission.

Simon and Zurko(1997) classify separation of duties into two main classes strong exclusion or static separation of duty and weak exclusion or dynamic separation of duty. Implementation of separation of duty during design/administration time known as static separation of duty or runtime which is known as dynamic separation of duty (Perelson and Botha, 2000). Static separation of duty permanently prevents the user from performing any tasks that are conflicting to tasks within his permission and does not change given under any circumstances. Dynamic separation of duty on the other hand prevents the exercise of permission when certain conditions exist. Therefore based on the context under which a transaction is being processed a user can be prevented from executing a task. Simon and Zurko(1997) further classifies dynamic separation of duties into simple dynamic, object based, operational, history based, order dependent and order independent dynamic separation of duty.

A benefit of implementing dynamic separation of duty is to prevent the execution of valid assigned roles and permissions within the same transaction if there is a conflict in any of these roles or permission. In other words, though permissions have been validly assigned, a subject cannot exercise these rights together in one transaction if they are seen to be conflicting. The risk in this approach is in cases where subjects have exercised validly assigned roles or permissions within different transactions at different times to perpetrate fraud. As a matter of fact subjects have used such mechanisms as a means of creating deception to commit fraud. An example of such a case is when a bank staff opens a fraudulent account and at a later date approves a fraudulent loan for the account and then performs a withdrawal transaction as occurred in the 2006 fraud case of Donald McKenzie in the Royal Bank of Scotland (British Broadcasting Corporation, 2006). Object based separation of duty seem to deal with this.

Object based separation of duties was first proposed by Nash and Poland (1990). Under this policy, users are allowed to perform a transaction if they are authorised to perform the task in question on a data item if they have not executed any other transaction upon that data item. This applies perfectly to a transaction voucher or cheque in the banking sector for instance where the voucher is the object. For example a clerk who has issued say a bankers draft to a customer cannot process the same draft when it is presented to the bank for processes. There are however risks that cannot be dealt with using this type of policy. For example it cannot deal with situations where customer accounts are the object. The problem is that unlike cheques which can be processed once, customer accounts are reusable therefore if this rule is enforced, users can only perform one transaction on an account. The implication would be that some accounts cannot be operated on when all the banking staff have performed one transaction on the account. Implementation of object separation of duties could however be modified to take into

consideration the level of conflict created due to the transaction history of a user on that account. Loock and Eloff (2005) modification to the Chinese wall security policy is a very practical means to determining the level of conflict between a current transaction that a user wants to perform and the transaction history of the user with respect to that customer account.

3.14.3 Rules of the Clark – Wilson Model

Central to the Clark – Wilson model is the classification of data elements. Data can be described either as an Unconstrained Data Item (UDI) or a Constrained Data Item (CDI). The Clark – Wilson model also introduces the Integrity Verification Procedures (IVP).

Access control is between the subject, the data object (UDI) and the Transformation Procedure (TP) a concept known as the access control triple. The Clark – Wilson model revolves around 9 rules which are described as follows:

1. *The system will have an IVP for validating the integrity of any CDI.*
2. *Application of a TP to any CDI must maintain its integrity.*
3. *A CDI can only be changed by a TP.*
4. *Subjects can only initiate certain TPs on certain CDIs.*
5. *CW-triples must enforce an appropriate separation of duty policy on subjects.*
6. *Certain special TPs on UDIs can produce CDIs as output.*
7. *Each application of a TP must cause enough information to reconstruct it to be written to a special append-only CDI.*
8. *The system must authenticate subjects attempting to initiate a TP.*
9. *The system must let only special subjects (i.e., security officers) make changes to authorisation-related lists* (Anderson et al., 2001).

One other requirement which the Clark – Wilson model recommends is that TPs must be run serially for concurrency control and that CDI in the middle of a TP there is no requirement that the system is in a valid state. This requirement therefore demands that TP must be atomic as a key requirement in addition to separation of duty. That is to say that the whole TP must be completed or it will not be valid.

3.14.4 Role Based Access Controls

Role based access controls (RBAC) is a mandatory access control framework which attempts to match the functions/roles that members of an organisation perform within an organisation with the access granted to them (Farraiolo and Kuhn, 1992). RBAC is flexible in that it can take on organisational characteristics in terms of policy and organisational structure. It is seen as a framework which works well with other security policies taking advantage of their mechanisms for securing information.

The principle in RBAC is that users are made members of specific roles in line with the function in their organisation. Appropriate permissions are then assigned to the roles. These permissions are the actions that users require to take to enable them to perform functions assigned to them in their various capacities in organisations. Roles have been described as logical groupings of permissions that reflect a particular task that can be assigned to some user (Aziz et al., 2006). Permissions on the other hand are referred to by Aziz et al (2006) as representing actions capabilities applications or any kind of active behaviour that can be performed and to which we want to control authorization.

Role based access control provides the option to create a hierarchy of roles where roles can be composed of other roles. Hence sub-roles inherit all the permissions of the super-roles plus additional relevant permissions assigned to it. This gives the

opportunity to implement the principle of least privilege which has been seen as an important means in achieving integrity.

There are three basic rules in implementing role based access controls as described by Farraiolo and Kuhn (1992). These are:

1. Role assignment: A subject can execute a transaction only if the subject has been selected or been assigned a role. Transactions in this case are a transformation procedure therefore login is not classified as a transaction.
2. Role authorisation: A subject's active role must be authorised for the subject
3. Transaction authorisation: A subject can execute a transaction only if the transaction is authorised for the subject's active role.

In addition a role may be assigned more than one transaction and a user can be assigned more than one role. Transformation procedures are transactions in the Clark-Wilson. In that sense read only access which do not transform any data object can be implemented by defining various modes for data objects and assigning subjects the right to access the objects in read only mode using transactions.

In the process of implementing role based access controls there is the need to ensure that conflicting roles or permissions are not assigned to a user. In other words the administrators must ensure that the principle of separation of duty is strictly enforced to avoid situations where vulnerabilities which could be taken advantage of are created.

3.15 Cryptography, Protocols and Transaction Security

Cryptography refers to the science and art of designing ciphers with mathematical techniques. The focus of these techniques is to achieve information security objectives such as confidentiality, data integrity, entity authentication, and data origin

authentication (Menezes et al., 2001). Each cryptographic algorithm has its strengths and weaknesses hence they are used in concert to provide a complete suite of security services. Combined in a particular order, cryptographic tools form protocols which information security engineers use to protect systems against malicious use or errors. Protocols are therefore described as a series of steps, completed by two or more people designed to complete a task (Schneier, 2000).

Generally there are three main types of types of cryptography; symmetric asymmetric and hash functions. Each type of encryption has its advantages and use. Symmetric encryption, message authentication codes, public key encryption, hash function, digital signatures schemes and random number generation comprise the cryptographer's tool box (Schneier, 2000).

Symmetric/secret key encryption uses the same key for both encryption and decryption. It is therefore critical that the key is kept secret at both ends of the communication. Asymmetric/public key cryptography on the other hand uses one key for encryption and a different one for decryption. One of the keys is freely distributed whereas the other key is kept private. The freely distributed one is known as the public key whilst the private one is known as the private key. Asymmetric cryptographic algorithms are highly effective for integrity, authentication, and key distribution (Khun et al., 2001). When encryption is done with a public key only the intended recipient can decrypt the message using a private key. The intended recipient is the only person that can read the messages ensuring confidential communication (Anderson, 2001). Due to its computational cost public key encryption is normally used to exchange keys to be used for symmetric encryption (Weise, 2001).

Alternatively when encryption is done with the private key any recipient can decrypt the message with the public key but it ensures that only the private key owner could have sent the message. Hence this form is used to digitally sign messages (Khun et al., 2001).

A public key infrastructure serves as a platform for implementing an effective public key encryption system (Weise, 2001). It refers to a system of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A digital certificate is an electronic certificate that binds a pair of electronic keys to an identity. By certifying a person‘s public key it provides the assurance that electronic information communicated with the private-public key pair is authentic. Digital certificates are issued by Certification Authorities (CA) and it basically verifies a claim of a person to use a public key. Such mechanisms could tie an identity to a document a feature shown in chapter 5 to be critical in avoiding fraud. Driver’s licenses and passports should provide similar assurance in the physical world but the issuing authority and process is critical to avoid fraudulent certificates.

Digital certificates operate with digital signatures or encrypted message digest which is a hashed form of the message. The message digest serves as a digital fingerprint of the message. Alice encrypts with her private key and sends both the message and the digital signature to Bob. When Bob receives them, he decrypts the signature using Alice's public key, thus revealing the message digest. Bob verifies Alice’s public key using the digital certificate issued by a certification authority. To verify the message, Bob then hashes it with the same hash function Alice used and compares the result to the message digest received from Alice. If they are exactly equal, Bob can be confident that the message did indeed come from Alice and has not changed since it was signed.

If any part of the message is modified, the hash function returns a different result. Hash functions on the other hand employ mathematics to do irreversible encryption. They are designed to have the property such that it is not feasible to either find a message that hashes to a given value or to find two messages that hash to the same value.

Cryptographic protocols like the Secure Socket Layer/ Transport Layer Security (SSL/TLS), IPSec or Kerberos are used widely in electronic commerce transactions to ensure security. They are used to ensure secure communications; digitally sign and time stamp transaction to protect customer details, prevent non-repudiation and ensure that integrity of commercial transactions are maintained. The cryptographic toolbox could therefore be very useful in controlling fraud.

3.16 Security Modelling, Verification and Validation

A model in science is a physical, mathematical, or logical representation of a system of entities, phenomena, or processes. Basically a model is a simplified abstract view of the complex reality. In designing a complex system it is desirable to create a model for the purpose of analysis and to communicate the design.

In the effort to produce a suitable security for a system a model becomes a useful tool for analysis and for accurately representing the system that be used to solve the issue at stake. This is especially so because it is expensive to use real life systems. Models can be manipulated more cheaply, conveniently and with little risks to the organisation. Models at one extreme can be used to automate routine decision which has a characteristic of regularity while at the other extreme are used as tools for thinking (Pidd, 2004). The uses to which models are put to, whether for thinking or replacing decision making, are a result of the issues to be considered.

Aside analysis, models are also used to describe new or proposed systems it sometimes becomes necessary to show that the model can do what it says. This process of verification or validity of models could be done by informal or formal methods. A brief distinction between verification and validation is that verification is "building the system right", while validation is "building the right system".

Generally the main objective of performing a validation exercise is to test the correspondence between the policy and the requirements or model. This exercise deals with the system at the conceptual or logical level. It is known that a logical system expressive enough for mathematics is inherently undecided (Kuhn et al., 2002). This leaves two options for validation; to either reduce the system to make it decidable or to use human judgement. Validation is therefore an informal process and it addresses the questions whether the model designed can meet the requirements or the proof of correspondence between the policy and the system requirements. This is more so because in testing security models. The reason is that security testing focuses on proving the absence of undesirable behaviour rather than testing for design features and functionality. This presents a very difficult situation as there are always endless possibilities for failure.

On the other hand requirements specification could be done formally. The aim is to confirm proof of correspondence that the system, as described by the specification, establishes and preserves the properties in the requirements policy (Kuhn et al., 2003). If they are in a formal notation, rigorous proofs can be constructed, either manually or with machine assistance. Effectiveness of the model however would depend on the technology used to implement the solution. Hence the implementation of a model is

also critical to achieve the security requirements stated in the security requirements policy.

Though models of systems which are biased towards soft issues usually relating to social sciences/human behaviour are used for brainstorming and supporting decisions and require informal methods for validation. On the other hand models for more mechanical machine related systems can be used to automate routine decisions and its verification can be automated.

Security modelling in the rural banking systems especially for fraud control will be mostly deal with soft issues. This is due to two factors. Firstly it is because large segments of the problem are determined by socio-cultural factors which cannot be verified by automation. Secondly the study aims to design the right system for fraud control devoid of most implementation issues.

3.17 Fraud Identification and Control

Aside the generic models discussed earlier various specific fraud control mechanisms are available. Generally to undertake preventive control of fraud it is useful to be able to identify situations that indicate fraud. Fraud seems to be characterised by certain externally visible symptoms. According to Albrecht et al (2003) they can be divided into six categories: (1) document or record symptoms, (2) analytical symptoms---things that are too large, too small, unusual or out of the ordinary, (3) internal control symptoms---overrides of internal controls, (4) lifestyle symptoms---increases in lifestyle or exorbitant spending, (5) behavioural symptoms---changes in one's behaviour to cope with the stress of being dishonest, and (6) tips and complaints (Albrecht et al., 2003). Based on the above symptoms a search was done by Albrecht et

al (2003) of a database of 16 years of bank records from Microfiche and Corporate databases was made. The following results were found. The frequencies of occurrence of fraud with the above symptoms have been described below;

- *Exception reports, reflecting fraudulent transactions that exhibited unusual, atypical and otherwise questionable patters of supervisor overrides, transactions with no apparent business purpose, and transactions involving unusually large amounts. This symptom came from internally used bank records and occurred at least 221 times.*
- *Journal vouchers containing only one signature or incorrect information and/or reflecting transfers between different customers' accounts. This symptom was found on internally used bank records and occurred at least 22 times.*
- *Deposit slips completed by the fraud perpetrator with missing information, incomplete customer names or where the name of the depositor did not match the name on the passbook and/or the account name in the bank's records. This symptom was found on internally used bank records and occurred at least 56 times.*
- *Deposits and withdrawals exceeding $5,000 in the perpetrator's passbook account. This symptom was found on internally used bank records and occurred at last 90 times.*
- *Withdrawal vouchers completed by the fraud perpetrator missing customer names or signatures and/or containing incomplete or inaccurate information. This symptom was found on internally used bank records and occurred at least 35 times.*

- *Bank checks reflecting transfers between different customers' accounts or checks with altered dates. This symptom was found on internally used bank records and occurred at least 22 times.*
- *Withdrawal vouchers and checks containing purported customer signatures by the fraud perpetrator readily distinguishable upon comparison from the customer's signature. This symptom was found on internally used bank records and occurred at least 73 times.*
- *Withdrawal vouchers completed by the perpetrator showing a different name from the account name. This symptom occurred on internally used bank records and occurred at least 60 times.*
- *Large negative available balances in slush and other customer accounts. This symptom was found on internally used bank records and occurred at least 15 times.*
- *Split deposits of customer funds between accounts of different customers and/or deposits of customer checks where the fraud perpetrator received cash back. This symptom was found on internally used bank records and occurred at least 9 times.*
- *CDs closed prematurely with proceeds placed in lower interest-bearing passbook accounts, sometimes with large penalties. This symptom was found on internally used bank records and occurred at least 42 times.*
- *Customers not being present when accounts were opened and closed or when transactions were affected in the account. This symptom occurred on internally used bank records and occurred numerous times in 26 different slush accounts.*

- *Large withdrawals of cash by the fraud perpetrator from customer accounts. This symptom was found on internally used bank records and occurred at least 221 times.*
- *The mailing of customer account statements to the fraud perpetrator's home instead of to the customer, without written authorization. This symptom was found on internally used bank records and occurred in at least 40 different accounts.* (Albrecht and Albrecht, 2006).

Even though good screening practices can always be used to keep risky people out of an organisation, new motivation to commit fraud can arise and the character of people who have been admitted into an organisation can change. These fraud promoting conditions cannot be entirely controlled hence they must be observed. Mechanisms that remove the opportunity and prevent people from committing fraud can however be implemented and controlled to prevent people who might have a reason to commit fraud incapable of doing so. In designing an antifraud system the focus should be on implementing controls in such a way that the opportunity to commit fraud is reduced. It is important to include mechanisms that deal with or prevent symptoms and ensure for example that there are genuine source documents and that these controls cannot be overridden. Unusual parameters like large amounts could be used as an indicator for detection. Employee lifestyle, change in behaviour and tip offs could be indicators of fraud as indicated earlier and so mechanism must be put in place to investigate them. Detecting such symptoms however cannot be designed into the service delivery processes.

Really large frauds cases, over a billion dollars, have involved lax internal controls (Anderson, 2001). The general view is that good fraud control comes in the form of

better management, control and audited access of employees, partners and customers control systems (Small, 2004). A theme identified by (Foundation of Research and Education, 2005) as a good control of fraud is to build standardised and accepted management practices and processes that are aligned with new technology. Though it is desirable to align the fraud control system with technology, their standardisation could reduce their impact since fraudsters use highly dynamic techniques as discussed earlier. It is therefore preferable to have systems that are tailored to the circumstances of the organisation in question and capable to the changing threat situation. Systems that usually rely on technology are inflexible whereas people dependent systems can be regularly configured to reflect changing risks and are more responsive than static systems (Foley, 2003). To achieve the level of dynamism that is able to deal with fraud it would be desirable to use technology but retain some level of human configuration.

Foley (2003) further states that Systems among others must be designed to be resilient to infrastructure failures and to achieve this, designs must be flexible enough to deal with the changing risk and fraud environment. Proactive forensic data analysis tools like sophisticated analytic testing, computer-based cross matching, and non-obvious relationship identification can be important in the detection of fraud (KPMG, 2007). This can help identify potential fraud and misconduct that otherwise would remain unnoticed by management, possibly for years. Some of these tools are however post-transaction where detection occurs when the fraudster could be long gone. Detection and prevention in a timely manner more desirable because it makes good business sense and can provide cost savings by minimizing the resulting damage (Deloitte Development LLC, 2004).

Fraud detection systems usually use intrusion detection mechanisms (Kvarnstrom et al., 2000). Intrusion detection involves techniques that are used to detect events in a system that violates a security policy. One of the main problems using intrusion detection methods for fraud detection is that fraud involves a deliberate attempt to mislead, and so fraud instances that do not violate security policies might not be detected. This is a particular problem in anomaly based detection where normal system behaviour does not necessarily indicate the absence of fraud. Traditionally intrusion detection of undesired activities in an information system is done either through the use of signatures of the undesired activities, detection of an anomalous situation or the use of state patterns. Pattern based detection depends on knowing the characteristics of the undesired activity. On the other hand anomalous behaviour depends on knowing the characteristics of normal behaviour of the system without any undesired activity (Kumar, 1995).

Detection based on signatures is done through the use of matching signatures to observed events. Signatures are patterns of known undesired activity. Signature based detection is very rigid and could be very reliable in detection in some cases. There are some problems that arise with using signature based detection. First there can be a high level of high false positives especially in simple pattern matching as is done in signature based detection (Cisco, 2002). The second problem is that when an attack does not match exactly the signature the fraud can be missed. Another problem that arises in using signatures to prevent fraud is that fraud is highly dynamic with many variations for deception hence each case of fraud is a rare incident. Also as discussed earlier historical incidents which can be used to create signatures are not very good pointers to future incidents.

Anomalous based detection on the other hand is able to detect previously unknown attacks and detection is highly dependent on the system learning what is normal. The problem with this kind of detection method for fraud however is that networks can be isolated in the case of intrusion detection to ensure that no undesired activity is done. One can never be sure that the supposedly normal state is devoid of fraud or that users cannot use "normal" processes to commit fraud.

It is clear that both techniques involve the use of a current activity being inside or outside a set of predetermined set. The problem with both approaches is that it depends on prior knowledge of how a fraud should look like and does not make use of possible vulnerabilities a system might have. A vulnerability analysis looking at weak points in the system is necessary to bridge these two forms of detection. This would cover known and unknown fraud patterns and unacceptable transaction patterns which could result in fraud based on vulnerabilities and weaknesses of the system.

3.18 Banking Systems and Banking Controls

Currently there are a number of banking controls that are used to control fraud. These involve the physical and electronic controls that are implemented to forestall in this case any operational risks. This involves protecting the banking operations. A banks operations involve a branch bookkeeping system comprising customer account master files and a number of journals that record and keep track of day to day transactions (Head, 1966). The main threat to this system is thought to be the bank's own staff. There are also high-value messaging systems behind the scenes that move large sums of money between banks locally or internationally. These systems are used to trade securities, to issue letters of credit and guarantees among others. Banking systems are generally protected by bookkeeping mechanisms. In addition, access control

mechanisms and cryptographic mechanisms are also used to support the protection of these systems especially in area of interbank messaging systems (Anderson, 2001).

Banks also use physical security mechanisms like safes and vaults with burglar alarms with cryptographically protected messaging system linked to control centres run by security companies.

Recently most banks have an online presence which gives customers the ability to manage accounts and perform some transactions on the internet. They integrate back into main bookkeeping systems of banks and traders. These systems require secure communications between the customer and the bank and or merchant usually secure socket layer/transport layer security (SSL/TLS).

Generally banking information systems serve two purpose of providing real time responses to enquiries about individual account status and providing more complex combination of information for management (Head, 1966). A typical banking system has various data structures usually an account master containing each customers current balance and previous transactions covering a period of say 90 days, a number of journals tracking assets which are going through the system (Anderson, 2001). It also has various journals which hold transactions from teller stations, cash machines check sorters etc but which have not yet been entered into the ledgers and finally audit trails recording which staff member did what and when.

Vulnerabilities within these banking systems enable fraudsters to commit frauds such as rogue trading, fraudulent loans, wire/transfer fraud, forging documents to commit fraud and identity theft. Other frauds like including forged or altered or stolen cheques, cheques kiting, payment card fraud, impersonation or identity theft, prime bank fraud,

fictitious bank inspector fraud, phishing and money laundering have been committed (Henderson, 2000).

3.18.1 Customer Identity and Identity Crime

Arguably the most important issue in banking security is identity management. This is because a person's identity is central to almost all commercial activity. Identity is however a social and personal construct (Fearon, 1999). It involves marking the person by a set of distinguishing characteristics which are socially consequential but more-or-less unchangeable. Social identity therefore involves a set of persons marked by a label and distinguished by rules deciding membership and characteristic features or attributes. Though certain categories of identity in current usage are not seen as central to a person's identity, identity however evokes the idea that social categories are bound up with the bases of an individual's self-respect (Fearon, 1999).

Banks open accounts for legal entities that have the capacity to enter into a contract and can be held liable in the event of a breach. To distinguish an individual is to identify an individual (McCallister et al., 2009). To do this organisations use a collection of personal information that commences at birth, expands throughout life and terminates upon death to create and verify identity (CIFAS, 2009 , Fafinski, 2005). Identity in that sense describes a data construct or a series of attributes that represents an actual entity in a particular context and by extension an identifier is simply data signifying an identity (Office of the Corporate Chief Information Officer, 2003). This information arises in two ways; biologically and socially (Grant, 2007).These include personal details such as a person's name, date of birth, address, mother's maiden name etc. Each piece of information forms a partial identity of an individual and each personal identifiable information or a combination of such information can distinguish an

individual to an extent (McCallister et al., 2009). These details are in turn verified by a mosaic of documents and records, including passports, driving licences, birth or marriage certificates, utility bills, bank statements, payslips, educational qualifications. To use this form of identification requires reliable systems that can produce such documents and records.

Identity crime is a generic term covering identity theft and identity fraud. It is used to describe a crime in which a perpetrator uses a false identity to facilitate the commission of a crime like fraud (Police Commissioners' Conference-Electronic Crime Steering Committee, 2003). A false identity involves creating a fictitious identity by manufacturing, forging or fraudulently obtaining legitimate documentation to satisfy proof of identity requirements. It also includes altering one's personal identifiable information. Identity theft on the other hand occurs when the perpetrator uses the personal identifiable information of another living or dead person. Bruce Schneier (2005) has referred to identity theft as an oxymoron because identity is the one thing that cannot be stolen and that identity is not a possession that can be acquired or lost.

The actual crime that occurs in identity theft is fraud through the use of impersonation (Schneier, 2005a). Identity fraud occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.

Identity crime has however gained currency in recent times mainly because of the increase use of information-based credentials. There are two issues that arise as a result of identity theft. These are access to personal identifiable information which raises privacy issues and the second is the ability to use this acquired personal identifiable information to deceive another person. Most often solutions have focused on achieving

privacy (McCallister et al., 2009) even though the problem is to do with one person using another person's identity to create deception.

To control this organisations use of robust controls to ensure that users are who they say they are and they can only see the information they are authorized to see (PricewWaterhouseCoopers, 2004). It also ensures that identities are set up on systems when people join and deleted when they leave an organisation in an efficient and prompt manner. Properly identifying customers when they open accounts in a bank is very crucial and a key part of customer due diligence in banking. It is commonly accepted in banking that customer due diligence popularly known as Know-Your-Customer (KYC) is key to ensuring security of banking operations and the prevention of the use of banking facilities to engage in criminal activity and money laundering. The Bank for international settlements indicates that KYC policies should involve a customer acceptance policy, customer identification, an on-going monitoring of high risk accounts and risk management (Working Group on Crossborder Banking, 2001 , WGCB, 2001). A customer acceptance policy is essentially a policy on customer profiling involving how to identify high risk customers and deal with them. An important part of a carrying out a customer acceptance policy is customer identification and this forms part of the identity management process.

The processes involved in identity management are the creation, management and deletion of identities of users within an organisation. To create an identity, most organisations rely on identity credentials packaged by another party and presented by the person who is requesting to be a member of the organisation. The problem is that the initial identity credentials presented by a person to create an identity could be

fictitious hence there is the need for business institutions including banking organisations to adopt mechanisms that are reliable to prove the identity of a person.

There are therefore three parties involved in creating an identity. These are the subject, the accrediting party and the relying party(Lowry, 2003). The first step is for the accrediting party to verify the identity of the subject. This involves proving that the individual is who he says he is. In other words the unchangeable personal identification information for which society identifies the subject must be shown to be true. When the identity is verified a credential must be created and packaged. The credential must be such that the relying party can trust it. This requires that the credential be reliable and that it proves that the bearer is the true owner of the personal identification information.

Two main issues are important to ensure the reliability accreditation process. The first is whether the accrediting party has reliable information to certify the subject's identity. Secondly, the form of packaging of the credential awarded to the subject for presentation must also be such that it is reliable. The credential package must be such that it is difficult to forge, clone, alter or the subject cannot be impersonated (Working Group on Crossborder Banking, 2001). The best ways to deal with these problems depend on the context and the environment within which the parties are operating and the accreditation is being done. Grant (2007) indicates that it is important to have the accrediting authority accept liability for certifying the identities of person and for creating an audit trail for the purpose of traceability.

3.18.2 Customer Authentication

When an identity has been created in an organisation, the issue of verifying their identity when they return arises. This involves a process where the person professes an identity usually issued by the company and presents an identifier or some credentials.

This identity credential forms the basis for determining different levels of service use for users. It is the main reason a fraudster would want to assume the identity of another person to receive his level of service. Customer authentication is therefore very important. It refers to the process by which a subject is recognised and this is when the presented identity is verified and accepted to be valid (Stewart et al., 2005). Computer systems usually do not know one person from another so what a computer would typically verify is the credentials presented to it by the subject. One of the mechanisms which organisations use in the management of identities is a digital identity. This involves the codification of personal identification information and to assign a unique identifier for which the computer system can use for the purpose of authenticating the natural person in a computer system.

There are three main forms of verifying an identity in authentication (Stewart et al., 2005). The first is "what a person knows" for example a PIN or password. The second is based on "what on what a person has" for example a smartcard. The third form of authentication is based on "who the person is" which is a biometric factor like a fingerprint or iris pattern. In addition to these there can also be authentication based on "something you do" or "somewhere you are" in terms of location. These means of authentication can be combined to increase the security.

In banking, PIN's are normally used a for identity authentication for Automated Teller Machines, online banking and point of sale transactions. They are usually a four number digit with each number ranging from 0 to 9. This gives 10,000 possible combinations of PINs and a 10^4 (0.001) probability of successfully guessing a PIN. PIN's can be used multiple times until it is actively changed by the user. They are usually used together with other authentication mechanisms to form a two factor

authentication system. This could either be with a chip, a username, a password or a Transaction Authentication Number (TAN). TAN's are one time use passwords that are invalidated when used. Its current use in Europe is in online transactions where is it used together with a PIN to validate transaction. Though various two factor authentication systems using PIN's seems to have drawbacks (Wiesmaier et al., 2005 , Bond and ski, 2003), it offers a secure authentication mechanism in reducing face to face fraud (Association for Payment Clearing Services, 2007).

In modern banking, the token used are credit or debit cards. A requirement of a token is that is must have a unique identity. Bank cards therefore have unique numbers and in some cases have a magnetic strip or chip. Bank card numbers are ISO 7812 numbers hence follow a convention (The Fraud Practice, 2008b). The first digit represents the Major Industry Identifier (MII). The next six digit is known as the Bank Identification Number (BIN) or recently Issuer Identifier Number (IIN) with access to the BIN or IIN a merchant has an opportunity to check if the card issuing bank is in the same country as the transaction. The BIN or IIN is then followed by an account number. The last digit is derived using the Luhn algorithm a checksum usually used to validate card identification numbers. The use of card numbers give merchants the opportunity to identify the origin of the card and when compared to say the billing address they can make a decision as to how risky the transaction is or whether it requires further investigation. Credit and debit cards also have the Card CV number which is the three digit number found on the signature strip of the card. Card can therefore be accurately identified but the way the information is used or checked and verified could determine how useful it is in deterring fraud. The problem with the identifier of banks cards is that it does not change so it can be copied when fraudsters get access to it.

Biometric identification, the third factor, involves a pattern-recognition mechanism that recognises a person based on a feature derived from a specific physiological or behavioural characteristic that the person possesses (Delac and Grgic, 2004). Involves the use of unique personal characteristics of an individual to identify and distinguish them from another person. These characteristics include fingerprints, retinal scans, DNA, voiceprints and facial characteristics. The difficulty in using this measure is that criminals can use another person's identity and their own biometrics to set up a fraudulent account from the start and can be difficult to detect if the bank does not have a record of the persons biometric information. The attractiveness of biometrics which is its difficulty to change is also a disadvantage. However when it gets into unauthorised hands it cannot be cancelled and reissued. It can however be very useful when the initial identification is correct. In using biometrics banks can match an identity to a natural person and this can prevent the person from assuming any other identity.

3.18.3 Transaction Authorisation

In certain cases an authorisation is required before a withdrawal or purchase transaction can proceed. This usually involves verifying that there is enough money to cover a withdrawal or transaction at the time it is processed and that the card used has not been reported as lost or stolen (The Fraud Practice, 2008c). Seeking authorisations gives a merchant the all clear to process then transaction**.** An authorisation does not guarantee that a transaction is not fraudulent (UK Card Association, 2009). This is because the checks are limited and does not do a wide range of checks to prevent deception.

3.18.4 Cheque verification

Merchants can cross check with a bank to verify if a cheque is valid or not. Typically cheque verification can provide information about an account that can help a merchant

to make a decision to stop a transaction. Information about an account that can be verified include the account number or the routing number (The fraud Practice, 2008a). If any of these details are found to be invalid the transaction cannot go ahead. On the other hand if the account is currently in a non-sufficient funds balance position to cover the cost of the transaction it cannot go through. Also when instructions like a stop payment order for the cheque number being used for the purchase or account is given by the account holder, it would be revealed during verification and the transaction would be stopped. Finally if the account is a non demand deposit account, closed or does not exist it or whether the cheque is stolen, forged or fraudulent it would be disclosed and so payment cannot go through.

Cheque verification processes can verify that the details on the cheque and also prevent a transaction to be processed if there is insufficient funds in the account. It is not an effective fraud detection mechanism because it cannot detect a forged cheque which has correct account details on it.

3.19 Summary

Analysis in this chapter has revealed various issues that must be taken into consideration in managing fraud risks especially in rural banking.

Information security techniques could be used to enforced internal controls and it should therefore be seen as a tool that can be effective in implementing internal controls. Security however is said to be like a layered onion: on the outside are the users, further inside is the relation between user and system and between system, further inside is the software that enforce security rules and in the centre is cryptography that enforce security (Schneier, 2000). Security is never simple and it is

more than a series of counter measures rather it is a complex system that interacts with itself, the assets being protected, and the surrounding environment (Schneier, 2006). These interactions affect security in a profound way in that they are the points at which the systems fails when attacked. Security systems have multiple stakeholders with each stakeholder having an agenda which might not necessarily be in line with the others. For the mechanisms aimed at achieving the security objective to succeed, the stakeholder made responsible for enforcing it must be in line with their vested interest.

It is very important that the context within which the organisation operates must be taken in to consideration in designing effective controls and that fraud risks must also be managed in compliance with business goals. To achieve the most effective controls, the system must be looked at holistically. It is important that the human context within which the technology is going to operate is not be sidelined. It is also important the controls put in place are responsive and adaptive. To achieve that it is important to have some level of human configuration for the system to maintain the flexibility. Though risk mitigating mechanisms could be inspired by standards and best practices, they must be modified to fit the organisation in which they are to be deployed and how the various stakeholder goals are aligned.

Also shown in this chapter are several security models available to achieving various security goals within a business system and to put together into an access control system to controlled access to resources.

The next Chapter explores the issue of human behaviour and culture in security systems.

Chapter 4

4 Information Systems Security and Culture Interactions

This chapter discusses issues relating to culture and security interactions. It first discusses the social component of information systems. It then looks at the types of culture and how they might affect success of technological change and security systems. There is subsequently a look at the culture of Ghana and how it might affect the success of any security system implemented to deal with any fraud risks within the rural banking industry.

4.1 Social Dimension of Information Systems

Information systems are made up of information stored or processed by an organisation, the hardware and software that constitute system configuration and procedures that guide user actions and people. Besides a structural view, there is a functional view of systems which is in terms of its inputs, processes and outputs of material, energy or information. There is also a set of relationships between various parts of a system creating functional as well as structural relationships with each other. The interaction between the various components of an information system creates a

culture within an organisation which has an impact on security (Veiga and Eloff, 2010). This perspective indicates the presence of a technical part but also a social dimension which arises as a result of the interaction between users. In that sense information systems have a social system that is formed by the actions and relations among the users (Karyda et al., 2005). These elements of information systems should be taken into consideration in designing controls. This is because organisational issues like the loss of organisational memory and the lack of community mechanisms and changing threat environments are not just a contributory factor in security failure they can often be the primary cause (Anderson, 2001).

4.2 Culture and Technology Interactions

Both cultural determinism and technological determinism are perceived to be unsuccessful in the management of technological change (Jackson and Philip, 2010). Technological determinism takes the view that technology is the key determinant for driving cultural change and bringing about techno-change success and that change can be planned and implemented in a top-down fashion by senior management. This approach lacks the attention to culture. On the contrary cultural determinism takes the view that the main cause of techno-change failure is the neglect of human and cultural factors and that the major causes of resistance are factors inherent in people either as individuals or in groups. There is therefore an attempt to radically change organisational culture prior to IT implementation in an attempt to achieve successful introduction of technology. From this perspective, the major causes of resistance are factors inherent in people and groups. In cultural determinism, culture is viewed as behaviour that cultivated, manipulated and controlled by management (Veiga and Eloff, 2010). This approach therefore lacks attention to technological issues like

deriving requirements developing technologies suitable to existing culture. Aligning technology and culture to each other could be a more successful approach.

4.3 Human Behaviour and its Influence on Security

A variety of reasons and explanations have been put forth for explaining the lack of effectiveness in the use of IS security policies. Whereas the security objectives for individual entities like servers, workstations, files and networks are similar across different organisations, there is no single security solution, nor a single security policy that can fit all organisations. The indication is that the human factor and context affects the success or otherwise of an information security system. In order to be effective there is the need to align security requirements, organisational goals and other stakeholder objectives that depend on the specific organisation and its environment.

In attempting to understanding the influence of the human factor it is important to recognise that people are more than just the roles that embody their work identity for example an accountant. Each individual also has a unique set of attitudes, beliefs and perceptions (Ashenden, 2008). These attitudes could affect security in a profound way. It is always said that the strength of the security of a system is dependent on the weakest link and humans are said to be the weakest link.

One reason often cited includes the view that security controls often constitute a ‘barrier to progress’. This view indicates an antagonistic view of human security interaction which would result in security policies being circumvented by employees in their effort to perform their tasks efficiently. The impact of social element on information security makes it more imperative for information systems to take internal control systems on board since they are designed to deal with weaknesses inherent in

humans. In the eight principles of information security one of the principles cited is that information security is constrained by societal factors (Swanson and Guttman, 1996). It indicates that the ability of security to support the mission of an organisation may be limited by various factors, such as social issues. It however admits that the relationship between security and societal norms is not necessarily antagonistic. Although it admits that security can in some cases help meet societal goals like increase the achievement of privacy goals, the general view is that societal factors only limit the ability to achieve desirable security.

Security however is not always constrained by societal factors it can be enhanced by societal factors. The vigilance and the willingness of a community to cooperate with police for instance is a critical factor in the success of police investigations hence the character and culture of a community is a crucial factor for a security measure to succeed or not. Reliable controls can only be achieved by understanding the failure modes of the system and most of these are a result of human failures. The success of many attacks on computer systems can be traced back to the security engineers not understanding the psychology of the system users they meant to protect (Stajano and Wilson, 2009). This further shows the need to consider culture in the design of systems.

Social factors can affect security mainly in two ways. They do so by thwarting or supporting the implementation and management of security systems. They also do so by being exploited by the attackers to achieve their ends. The latter is known as a social engineering attack. It is worth noting that the difference between these two is about who takes advantage of human characteristics; the security manager/designer or the attacker. Whatever the case is, it is important for the security manager to understand the nature of humans.

4.4 Social Engineering

The exploitation of human weaknesses by attackers to breach IT security has recently become a topical issue. This involves someone manipulating others into revealing information that can be used to steal data, access money, information on computer systems, phones, or even an identity (Peltier, 2006). Social engineering attacks are the most difficult to prevent mostly because they are not predictable and are based on the manipulation of humans who tend to be illogical and unpredictable. According to Peltier (2006) the goal of the social engineer is to prey on the attributes of humans such as the desire to help others, the tendency to trust people, the fear of getting into trouble and their willingness to cut corners. Social engineering therefore uses human and social characteristics to aid an attacker.

Social engineering attacks usually involve two elements: the physical aspect and the psychological aspect (Orgill et al., 2004). The physical aspect makes use of location where victims have a false sense of security whereas the psychological aspects prey on the human nature and emotion. Most often social engineering attacks combine these two aspects in a single attack.

An audit conducted by Orgill et al (2004) showed that solitary employees were more easily manipulated than those in groups though peer pressure could sometimes be detrimental. Building trust between the victim and the attacker was vital for a successful attack. Education of would be victims is seen as the main method of preventing such attacks.

It is also worth noting that in these attacks the behaviour of people is not changed, rather they are exploited. This is an important hint for security system designers and

managers to understand the behaviour of users to help set up more robust systems and to help educate them.

4.5 Human Behaviour and Culture

Culture has been described as the customs, ideas and social behaviour of a group of people (Oxford University Press, 2002). It describes the set of shared attitudes, values, goals, and practices that characterises an institution, organisation or group. National culture has been defined as the programming of the mind that is manifested in the values and beliefs of a society (Hofstede, 1980). Values are reflected in an individual's preferences for certain states of affairs. There are two main cultures that comes to the fore when discussion its impact on information security. There is the culture within the organisation and then the culture within the larger community outside the organisation. In an organisation an individual's cultural conditioning would come together with their interactions to determine their way of life how they react to technological solutions. Individuals have a personal and social culture that they bring with them to work (Ashenden, 2008). This further indicates the importance of not only the internal culture of an organisation but also its external culture and character.

The main levels of organisational culture has been described artifacts, espoused values and shared tacit assumption (Niekerk and Solms, 2009). Artifacts are what can be observed, seen, heard and felt whilst espoused values consist of the organisation's official viewpoints usually expressed in mission statements etc. Shared tacit values are assumptions beliefs, and values that have become shared acquired from a joint learning process. Shared tacit values are usually taken for granted in an organisation. Though organisations may have some control over the culture within the organisation it does

not have much control on the culture outside it. This however should not make it any less important.

Security problems are shaped by the outer and the inner context of an organisation (Karyda et al., 2005). Whilst the outer context includes factors that are found in the economic, political, social, competitive and industrial environment of the organisation, the inner context on the other hand includes structural, political and cultural elements within the organisation. Both the outer and inner context determines the nature of the organisation. These two contexts shape the outcome of processes through the activities and behaviour of the actors. In developing and implementing policies it is important to understand the emergent, situational and holistic features of the processes within the context of their occurrence in order to find the appropriate policy.

4.6 Taking Advantage of Culture in Security Design

It is suggested that the type of culture that a group has determines the effectiveness of controls. The argument is that social interaction gives a world view of an individual and this combines with the individual's cultural bias which in turn determines a person's way of life (Jackson and Philip, 2010). Figure 4.1 shows the four classes of social positions that a person could be classified as.

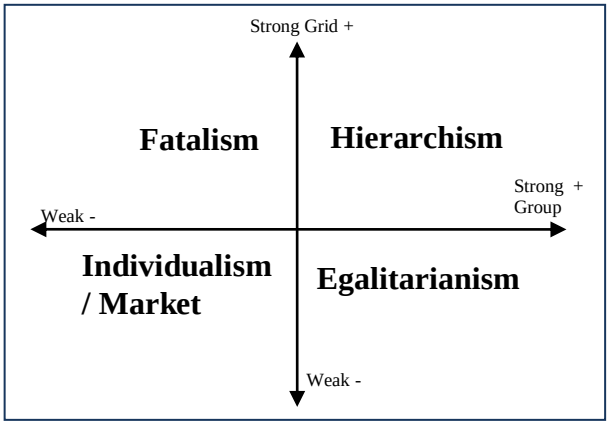


Figure 4.1 Cultural Theory and the four ways of life (Jackson and Philip, 2010)

The four types of social characteristics are determined by the level of two dimensions grid and group (Jackson and Philip, 2010). Whilst grid refers to the extent to which an individual's life is governed by rules and regulations, group individual are controlled by the group in which they live or work members and are compelled to act in accordance with the collective interests of the group.

Fatalism is characterised by strong grid and weak group. People in this group display values of apathy and fear. Hierarchism is characterised by strong grid and strong group and emphasis on order, discipline and coordination of tasks to ensure that events stay on course. Individualism/market offers ample opportunity for creativity and innovation. Egalitarianism is characterised by group concerns which take priority over individual interests stressing the importance of group-ethos, teamwork and trust.

There are other views proposing a four dimension model of work-related culture (Hofstede, 1980). These are power distance, uncertainty avoidance, individualism and masculinity. It is suggested that the appropriateness of, or preference for specific controls depends on the dimension that a group falls in.

Different cultural characteristics enable or hinder technological solutions. Whilst hierarchical culture could encourage visionary leadership and coordination of resources egalitarianism on the other hand could encourage teamwork trust and knowledge sharing. Individualists in contrast to collectivist are more inwardly focused and predisposed to thoughts and actions that benefit themselves over others in their peer group (Luo et al., 2009). Consequently their desires and perceived requirements for privacy are strong. Many organisational security activities like system and web traffic monitoring through proxy servers require some level of invasion of individual privacy. To achieve this there is the need to sacrifice some level of individual privacy in order to maintain organisational security. Questions about the extent to which an individual would forgo personal privacy to enhance organisational security arise. Individualism focuses on "I" but could encourage creativity, drive and innovation (Garcia-Sordo and Baren, 1999 , Jackson and Philip, 2010) but could hinder policies that invade privacy.

For collectivist employees, organisational motives are of greater importance than their personal goals and the use of monitoring controls is likely to strengthen their sense of affective commitment to the organisation as long as they believe the monitoring activity benefits the firm.

There is a suggestion that cultural values of the originators of some management and security systems underline these systems. These values might be significantly different from the values of the adopting countries and the difference in cultural values has been described as a potential barrier to implementing such systems (Al-Zamany et al., 2002). Models like the Clark-Wilson model and standards like that recommended by the Basel committee which were discussed in the last paragraph might not work in Ghana if they

are implemented in the same way they are in places like Europe and America. They should therefore be aligned to the culture of Ghana to ensure they are successful.

Jackson and Philip (2010) have argued that cultural and technology interactions that impact the success of technological change are not static and recommend using techno-cultural emergence as the most effective approach. That notwithstanding it is clear that the culture of a community must be thoroughly understood and that the design and implementation of a security system must be closely aligned with culture to ensure success.

4.7 Culture of Ghana

The values of the Ghanaian society is one set on social harmony and the well being of others not just the individual (Utley, 2009). There is a high attitude of social conformity and tribal loyalty which is in turn rooted in ancient tradition and religion. This makes for a close knitted society with clear rules and boundaries that affect interpersonal relationships, legal rights to property, social roles and obligations.

4.7.1 Tribal and Families Roles in Ghanaian Societies

Most individuals in Ghana belong to one ethnic group or the other and identify themselves as such, speak the language of their tribe and largely follow the traditions of their tribes (Utley, 2009). Tribes on the other hand are made up of families to which individuals belong to.

A Ghanaian family has been described as a cohesive unit which ideally provides economic (in terms of land for farming among others), social and psychological security to all its members (Degbey, 1997). The Ghanaian family defines social and moral norms and safeguards material and spiritual customs and traditions as well as

providing a variety of role models for preparing for adulthood. Mutual help, collective responsibility and reciprocal obligation are the important norms (Utley, 2009). This system with the dominance of its elderly members being a safe of society knowledge has a relatively high degree of social control on the individual especially the youth.

Families therefore form a very important community unit for identity and cohesion in rural Ghana. Families are the owners of land in Ghana and Chiefs and family heads are caretakers of land (Ubink, 2007) on behalf of their family members and this is an important source of family cohesion. When two individuals meet and decide to get married the families from both ends must come together to witness the ceremony to make it valid. Families are the ones who meet to contribute resources and arrange a funeral when an individual dies. Families also serve to mediate between two members when there is a problem, arrange to take care of an ill family member or offer support when a member gets into trouble. It is worth noting that the concept of a nuclear family is not popular in rural Ghana, rather extended family are the norm. Ghanaians trace their roots to their ancestral village for identity and even in death they are sent back there to be buried. Such a society provides a context which is very different from most western societies.

4.7.2 Family Reputation in Ghanaian Society

Families desire respect within their communities and it is the responsibility of family members to handle a misbehaving member who threatens by his actions to disgrace the family (Herndon, 2009). Badly behaved children are seen as a disgrace to the parents and any adult who witnesses a misbehaving child does not hesitate to admonish them and then take them to their parents for more of the same (Utley, 2009). A morally

upstanding Ghanaian is expected to dress well and shabby dressing in public for instance reflects poorly on the family.

There is further evidence of the importance of a family's reputation in the marriage process. When a man announces his intention to marry a woman for example, the woman's family would usually investigate the background of the family before they give their blessing (e-Harmony, 2009 , Salm and Falola, 2002). Some of the things they would look out for would be the reputation of the family. They would investigate to see that no immediate family member such as a sibling, an aunt or uncle is known to be a thief, prostitute or murderer or that there is no evidence of genetic disabilities or chronic illness in the family. They would also check to ensure the man is of good character and well matched to the bride and has no illegitimate children or has another marriage elsewhere. This is an incentive for families to maintain a good reputation.

Utley (2009) describes the communal values that enable information of misdemeanours and scandals committed by individuals to spread within the community. This is a situation that further dissuades members of the community from committing undesirable behaviour which might embarrass their families.

There is therefore the incentive for Ghanaian families to maintain their reputation. This character could be used to enhance fraud control since families do not want to be associated with bad behaviour like fraud.

4.7.3 Traditional Ghanaian Art

The Ghanaian concept of art differs from that of western cultures in terms of its importance to society (Salm and Falola, 2002). Whiles western art stirs emotion within the viewer Ghanaian art serves an aesthetic and functional purpose.

Ghanaian art is essential to society and symbolises all aspects of cultural and social life. It employs many levels of symbolism to show cultural and social structure and to depict the history, beliefs and values of the people. It acts as agents of communal and national unity. It comes in the form of textile, basketry, beads, leather work, sculpture and metal work. They are usually not separate from other forms of art like music. Ghanaian art link their aesthetic characteristic to their functional objectives like a performance or ceremony within a context like bereavement, a marriage or a birth. This feature of Ghanaian art could be adopted in modern day financial transactions.

An example of such art is the adinkra symbols which is a system of traditional aphorismic symbols (Salm and Falola, 2002). Originally used among the Akans of Ghana it is currently used by all Ghanaians. See Appendix F or www.adinkra.org for more samples of adinkra symbols. Adinkra is a set of symbols that express various themes that relate to the history, beliefs and philosophy of the Akans. They depict historical events, human behaviour and attitudes, animal behaviour, plant life forms and shapes of objects. They are currently used in jewellery, textiles, carvings and company logos among others. This is a Ghanaian art form that could be tapped to enhance fraud control.

4.8 Ghanaian Culture and Fraud Control

There is an indication that the Ghanaian society is collectivist or egalitarian where group/family benefit supersedes individual interest. This has a potential to facilitate fraud control or create risks. On the other hand if bank interests are aligned to family interest it could be used to enhance fraud control.

A possible risk that could be faced by a rural bank is that they could have members of the same family working in the bank. With a high level of family cohesion within such communities, there is a high risk of employees exhibiting loyalty to their family members within a bank as opposed to loyalty to the bank. The risk of having two conflicting users for example becomes higher reducing the effectiveness of separation of duty for the purpose of fraud prevention. This characteristic could also increase the motivation for a customer or an employee to bend the rules in order to benefit a family member. Aligning the goals of a family and the security goals of a rural bank could ensure a collective effort by the two towards fraud reduction.

Fraud control could also use art to promote anti fraud message just like corporate bodies currently use them to communicate their values. Alternatively some of the functional uses for which it has been put to for ages could be adopted for fraud prevention. It can be used to help bind or align a community to a fraud prevention system. Finally it could also be used to convey messages or codes which will only be understood by their users.

4.9 Summary

This chapter discussed the issue of culture in security. It pointed out that every information system has a social element that is a combination of both an internal culture but also a culture external to the organisation. It also showed neither that the lack of attention to culture or the view that failure is due to an inherent character of human cannot ensure successful implementation of technological systems. It also discussed the different social characteristics and its impact on the success of security systems.

Finally the culture of Ghana was discussed. The community and family structure and its art forms of Ghana were discussed. Also discussed was how cultural characteristics could be tapped to enhance or hinder a security of fraud prevention system.

The next chapter takes a closer look at the research methodology that was used to collect data in order to understand the rural banking industry in an effort to craft a fraud prevention system.

Chapter 5

5 Methodology

From the discussion done so far it is clear that to be able to obtain a desirable fraud control model it is important to understand the nature of the rural banking industry. What is important is to understand the context in which these banks operate. To understand the context a field research was done.

In this chapter a discussion of how the research was conducted is done. It covers the approach adopted for the research; it also discusses issues regarding the population studied how it was sampled. The methods used to collect and analyse data are discussed. It covers the methods used to collect which type of information and finally discusses how the information was analysed.

5.1 Approach of the research

The main theme of the research was that context is very important to achieve effective security. There was therefore the need to study the problem in such a way as to make culture visible. Various issues were considered to enable an understanding of the

context. Data collection was approached with the nature of operational risk and fraud in mind. As was shown in the previous chapters, the nature of operational risk and fraud is so varied and dynamic in its manifestation and that it can be manifest differently in different organisations. It is therefore not ideal to use conventional risk management mechanism that will lead to the focusing on some perceived serious threats neglecting the rest. This is especially so because there is no reliable record of previous fraud incidents to use as a guide and even if there were it would not be the most reliable means to predicting future cases. Also the problem of fraud is systemic and the profile of a fraudster fits many people.

With the nature of fraud, it was therefore not ideal to focus on some elements within the industry. The study of the rural banking industry was rather done holistically to have a broader view of the vulnerabilities in the system. The focus of the data collection was rather on identifying the systemic vulnerabilities than on transaction based vulnerabilities. Also since fraud is a result of failure in business processes the focus of the field research was on the banking processes. This approach was also used to help obtain a better understanding and to define the problems of the rural banking industry to ensure that designs can be made more resilient to threats. Several aspects of the industry were therefore studied to identify these vulnerabilities.

The research was also approached with the view that the rural banking industry is unique in nature. There was therefore an attempt to focus on the how its unique nature affects its operations especially the processes used to deliver the services it offers to the public.

Field research was chosen as the preferred means of data collection. This was to help obtain an in-depth understanding and explore the nature of the operations of rural

banking industry. This is because most research on the rural banking industry has usually focused on the impact of rural microfinance on poverty reduction and its impact on economic activity. It was therefore necessary to have firsthand knowledge of the day to day operations of rural banks. This approach was most desirable because of the focus on soft issues. The view taken was that quantitative and statistical approaches hide the soft cultural and contextual issues hence there was more use of qualitative data.

In this regard the field research sought to understand how the nature of the rural banking industry, the dynamics within the banks, its interaction with the rural communities and other stakeholders relate to fraud. To understand the entire industry the field research was structured to study the various organisations forming the rural banking system, their regulator and also to get other perspectives from the mainstream commercial banks. The groups of organisations studied included the rural banks, their sub regulator, ARB Apex bank, and the main stream commercial banks.

Though there were several hard issues to consider there were a lot more soft issues especially those issues cultural in nature which had to be taken into consideration in order to obtain a good security design. The bulk of the data collected was therefore mostly qualitative and unstructured. Also data collection was iterative incrementally collecting information to help understand the rural banking industry and to help develop a fraud control model.

5.2 Coverage of Field Research

Field research did not cover the entire country. Rather it covered rural banks in 6 out of the 10 regions. Various reasons accounted for the choice of these regions. Due to the level of detail that was required from the field study it was very time consuming and

expensive. There was therefore the need to use a small sample size. To be able ensure that the result holds for the population, a reduction in the size of the population was necessary. To achieve this it, was necessary to choose a more homogeneous population for which results from a small sample will hold true for the population. To attain this, a choice of six regions made. These were the Western, Central, Ashanti, Brong Ahafo, Greater Accra and Eastern regions. These regions were chosen due to historical and cultural similarity. They also had the bulk of the country's population and had the bulk of rural banks

Historically the Ghana (formally Gold Coast) was made up of four main regions (McLaughlin and Owusu-Ansah, 1994). The first was the coastal regions making up of the Western, Central, Eastern and greater Accra region. The second was the Ashanti region which is made up of present day Ashanti and Brong Ahafo regions. The third region was the northern territory which was made up of current day northern upper east and upper west regions. The final region is the Volta region which became part of current day Ghana after the First World War when the League of Nations split and mandated the German protectorate Togoland to Great Britain and France. See Table 5.1 below.

Colonial territory	**Current region**
Coastal region	Central
	Western
	Greater Accra
	Eastern
Ashanti	Brong Ahafo
	Ashanti
Northern	Upper east
	Northern
	Upper West
Togoland	Volta

Table 5.1 Historic and Current Regions of Ghana

The six regions chosen for the study are the coastal regions and Ashanti which the middle belt of the country. According to the last population census in 2000, the population in these regions formed about 74% of Ghana's total population (Ghana Statistical Services, 2005). These regions are mainly made up of Akan tribal grouping which form about 44% of Ghana's total population (Gocking, 2005) and 61% of population of the six regions. The Akans are made up of tribal grouping like the Bono, Akwamu, Asante (Ashanti), Akyem, Denkyira, and Fante. The other major tribal group in the six regions are the Ga-Adamgbe. The Akan tribal grouping have a relatively homogeneous culture, language, and authority structures (Owusu-Ansah, 1994). The basic unit in the Akan society is based on the matriclan system. In the matrilineal system, family lineage, inheritance and succession to wealth and to political offices and even basic relations within the village are determined by the relationship to the mothers and sisters. Though traditional leadership roles are mainly held by men, they acquire the positions through their relationship to the female members of the family. This system remains economically and politically important. Each lineage controls the land farmed by its members. It also functions as a religious unit in the veneration of its ancestors, supervises marriages and settles internal disputes among its members.

5.3 Organisations studied

For the field research, three main types of organisations were studied. First the rural banks were studied, and then the sub regulator, ARB Apex bank was, also studied. Finally the main stream commercial banks were also studied. Figure 5.1 Shows the organisation of the field study.

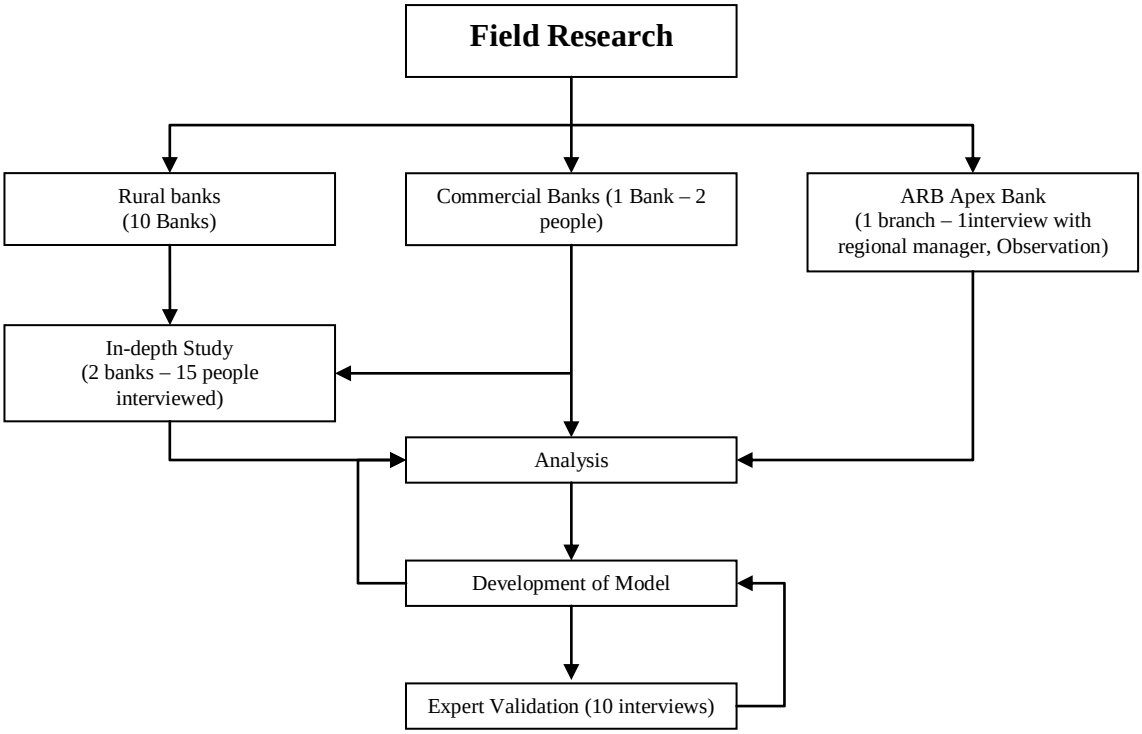


Figure 5.1 Field Research

In total ten rural banks were selected and studied due to assumed homogeneity discussed in section 5.2. This homogeneity was further confirmed from the consistency of the data collected. Two out of the ten rural banks were studied in more detail by observation. One branch of the ARB Apex bank and one commercial bank were studied. The details of the field study are discussed more subsequently.

Other informal contacts and interviews were done. This involved an informal interview with a former employee of a rural bank and some customers. Enquiries were made at the Registry of births and deaths and the Vehicle Examinations and Licensing Division on the process for obtaining a birth certificates and driver's license.

5.3.1 Rural banks

The rural banks studied were drawn from the coastal and middle belt. Table 5.2 shows the distribution of rural banks in the regions studied compared to other regions.

Region	Number of rural banks	Percentage
Southern and middle belt	104	80.6
Northern Ghana	14	10.9
Volta	11	8.5
Total	**129**	

Table 5.2 Distribution of Rural Banks by Segment of Country

This region has a total of 104 rural banks making a total of 401 agencies. A sample of 10 rural banks was selected representing 10% of the banks in those regions. The selected sample had a total of 50 agencies. Table 5.3 shows the sample taken and their respective regions.

Region	Sample Size
Western	2
Central	2
Eastern	1
Greater Accra	2
Brong Ahafo	1
Ashanti	2
Total	**10**

Table 5.3 Distribution of Questionnaire Sample

With the rural banks being the ones delivering banking services to the public, they were able to give information on the banking practices and the day to day operational activities in the industry. They were also the best organisation to provide information on threats in the industry. Also information on the structure of the banks, their interaction with each other, with the public and with the regulators was obtained from the rural banks.

5.3.2 Regulators

As discussed above the main regulator of banking in Ghana is the Bank of Ghana however there is also the ARB Apex bank which is the sub regulator. The ARB Apex Bank has a head office in Accra, five branches across the country and 7 clearing centres. Within the southern and middle belt there are three branches in Accra, Takoradi and Kumasi respectively.

One of the apex bank branches was studied during the field research. This study was in the form of an interview with the regional manager. Limited observation was also done. This was done to collect data about and understand the role and operations of the Apex Bank within the rural banking industry and their view of the rural banking system.

As mentioned earlier the ARB Apex bank regulates rural banking activities and also offers banking services like specie to the banks. They were useful in giving information about rural bank regulation in general and their role as regulators in particular. Being a regulator they also gave information on the regulatory regime, the rationale behind regulations and how it can help counter fraud risks. As the primary link between all rural banks they were also useful in giving information about the conduct of interbank transaction and the risks involved in interbank transactions. The ARB Apex bank also has a global view and could give a bird's eye view of the rural banking sector.

5.3.3 Commercial Banks

In order to understand the subject of banking in Ghana and what the industry standard is, it was necessary to contact bankers in the main stream commercial banking industry. Two bankers from one main stream commercial bank were interviewed. This was done after the initial survey of the rural banks and before the detailed study of the rural

banks. The commercial bankers interviewed were contacted a few more times for clarification and advice when certain issues arose.

Commercial banks are not considered part of the rural banking system and for that matter not part of the population that was being studied. This part of the field work proved valuable in helping obtain another perspective to the one presented by the rural banks. It also gave information and leads that helped in the conduct the data collection exercise from the rural banks. It was very useful in deciding what questions to ask and gave an informed perspective.

The commercial bankers also helped to understand the methods they use to control some of the common problems faced by the rural banks. It also yielded information on the banking processes used by these banks to deliver their services to the public. Studying the commercial banking organisation also gave the opportunity to compare the banking processes and controls. Information obtained was mostly used as input to shape the type of data/information to look out for especially during the personal observation stage of the data collection exercise.

5.4 Data Collection Methods and Administration

The data collection exercise was largely iterative. It collected data from the various respondents cyclically to aid understanding and incrementally develop and validate the resultant fraud control model. The data collection exercise made use of various data collection techniques. Methods used were a structured questionnaire, interviews, observation and document examination. The use of these different techniques was to benefit from the advantages of each technique.

As mentioned earlier the study of the rural banks was in two phases. The difference between the two phases was in the level of detail and the methods used. There were also some informal interviews. See table 5.4 for details.

Organisation	Position	Questionnaire	Interview	Informal Interview
Rural Bank	Chief executive	1		
	Manager	3	1	2
	Operations/Credit Officer	6	3	4
	Clerk		11	15
	Ex-Rural Bankers		2	4
ARB Apex Bank	Regional Manager		1	
Commercial Bank	Customer Relations Officer		2	7
ID Document Issuers	Electoral Commission/Vehicle examination and licensing department/Registry of births and deaths		3	
Total		**10**	**23**	**32**

Table 5.4 Data Collection

The first phase involved the collection of general information on the operations of the rural banks in terms of their organisational structure, internal controls, staffing levels, services and processes used to deliver these services. A structured questionnaire was used at this stage. See Appendix B for a sample questionnaire used. This phase covered the entire sample of all the 10 selected rural banks.

The questionnaire was administered face to face and it involved travelling around the southern sector of the country to the various rural to administer. This was to ensure a good response rate. Difficulty in contacting the various rural banks necessitated this mode of administration. They were answered by either the manager or the operations officer with the permission of the manager. They were used to collect general information about the banking structure, risks, control measures, source of risks and information about the roles of employees in bank. It was used to collect information to

help understand the fraud risks that rural banks are subject to. Information regarding the structure and the mechanics of the rural banking system were collected and analysed to understand how they operate. Information on internal controls that were already in place to deal with fraud risks was collected to look at how effective these controls are. The aim of this data was to gain an understanding of the systemic weaknesses that can allow fraud to occur. The information from the structured questionnaire also formed a good background on which interviews and observation was done.

The second phase was a more detailed study. It involved studying the dynamics of rural banking operations. Here 2 rural banks out of the original 10 were chosen for an in-depth observation and study. These banks were observed and their staff and managers interviewed to give further clarification about observations made. A total of 15 members of staff from the 2 banks were interviewed. The banks were observed and interviewed for a period of 4 weeks. This was to have as much detail as possible and to have an intimate understanding of the issues that come to play during their day to day operations. Observations made at this stage were discussed with the staff to gain a better understanding.

Interviews and observations were used to probe further and collect more information. This was to help thoroughly understand the nature of the risks and how they are manifested in the banking processes and any possibilities of mitigating them. The rural banking processes were studied to uncover how the systemic weaknesses could be manifested within those processes. In total 23 in-depth interviews were conducted. They comprised interviews with 15 employees of the rural banks with different roles. They included 1 manager, 3 operations officers and 11 clerks.

Aside the interviews and questionnaires administered to the rural bank, 2 commercial bankers and a regional manager of an ARB Apex Bank branch were interviewed. Interviews were also conducted with 2 ex-rural bankers, and 1 operative each from the electoral commission, registry of births and deaths and the vehicle examination and licensing division.

There were a total of 32 informal interviews iterative to collate the views of the various people. 10 of these interviews were to refine and validate the model using the expert views of 5 current rural banks. The rest were done to either help collect background information to design the research and or to seek clarification for various pieces of information collected earlier.

5.5 Information Collected

The views of employees and more detailed information about the banking process, reliability of controls and vulnerabilities existing in the system was found. Interviews and observations gave more new information than the structured questionnaire.

Employees from two rural banks were observed performing their day to day duties. Issues that indicated their attitude to security were observed. The ease with which non employees were allowed into the back office, the level of scrutiny of documents presented by a prospective customer were observed and discussed further with the employees to understand the true nature of the risk. The display of control and authority by managers and officers in the bank was also noted and discussed. Follow up questions were asked to explain issues if they were not understood properly.

Documents like application forms, vouchers, sample cheques, and banking procedures were studied. These documents were then discussed with employees to determine the

extent to which procedures for example were adhered to. Other things like the ability of forms and vouchers to force disclosure was also observed and discussed to understand the effectiveness of those documents in preventing fraud.

The field research was also aimed at collecting information on any other possible controls that could be used to deal with the risks. Various mechanisms devised by the rural banks and the employees to deal with risks they had identified were also noted.

Using a field research gave the opportunity to observe the operations of the banks to identify new information about their operations. It enabled the collection of information on the structure of the banking system and how the various parts relate to each other. The role of the employees and other stakeholder were studied since it is very important to help one understand the nature of fraud risks. The field research also gave the opportunity to interact face to face with these stakeholders and to ask follow up questions when the need arose. Details of the banking processes were closely studied.

Finally information on the nature of the communities in which the banks operate in was collected. These covered the peculiar characteristics of the communities that make it different from other communities and that might make implementing mainstream banking controls difficult.

5.6 Data Analysis

Data collected were presented in two main forms. Data collected from the questionnaire was codified and presented in bar graphs. These bar graphs were then interpreted to identify any trends and or predominant views. All the other qualitative data was presented in the form of discussions.

Information gathered from the field allowed building a structure of the rural banking system. It also allowed measuring the objectives of control against the banking mechanisms to identify the weaknesses within the system. A profile of the vulnerabilities and systemic weaknesses were then built. Banking processes were then analysed to see how the identified vulnerabilities could be exploited to commit fraud. A number of fraud scenarios were built with the help of the bankers interviewed to illustrate the problem. These fraud scenarios were made up of cases that were said to have occurred within the rural banking and the main stream banking systems. It also included other possible cases of fraud that could occur as a result of the weaknesses within the system.

Based on these scenarios and well known principles of system protection a model was designed to deal with fraud risks. The mechanisms adopted in the model were also discussed with banking officials to validate it.

5.7 Limitations of the Approach

There were a few limitations of the approach used. Since the approach adopted was to view the industry holistically there wasn't a lot of focus on how the various issues affect security individually in contrast to when they act with others.

Also the methods used were very demanding by their nature. This is because conversation and action occurred at the same time. There were many things that occurred very quickly as part of complex interaction among a number of persons. It was therefore difficult to observe and note what is said, to whom, in what way, with what effect, and the kind of behaviour at the same time.

Rural banks like many banks find it very difficult to discuss the issue of fraud. It was therefore very difficult to get the rural banks to discuss the issues and the mechanics of fraud. For instance it took so much time in the early stages of the field research to book an appointment and to administer the questionnaires face to face. It took up to four days to book an appointment to administer a questionnaire.

5.8 In summary

Due to the nature of fraud a holistic approach was adopted to study the rural banking industry. A field research was to collect information about the rural banking industry. An iterative process was used to collect information and to help develop and validate the resultant fraud model. A sample was selected from the southern and middle regions of Ghana for homogeneity and to ensure the best possible outcome of the field research. Also various data collection methods and instruments including a structured questionnaire, interview, observation and document examination were used to collect data. This was to take advantages of the various instruments and methods to help enhance the data collect exercise. The next chapter presents information collected from the field.

Chapter 6

6 Rural Banking Systemic Weaknesses

This chapter presents and discusses the findings of the field research. It discusses the weaknesses that exist in the rural banking industry that give opportunities to commit fraud. It discusses several systemic vulnerabilities in the rural banking system which is a result of the structure of the system, their operations and other soft issues that come into play within the bank and the community. The various issues discussed include services offered by the bank, Customer Identification, Staffing levels, Structure of rural banks and internal control in rural banks. It discusses the implication of these issues and its impact on controlling fraud.

6.1 Services Offered by Rural Banks

As mentioned earlier rural banks operate as commercial banks albeit offering fewer regular services than the main stream banks do. It was observed that a total of 14 services or products were offered to customers of rural banks. They generally accept deposits, offer lending and offer inward money transfer services. The accounts opened for customers are current and or savings accounts. They also offer investment tools like

fixed deposit and an avenue for customers to buy government bonds like treasury bills. They are however prohibited from performing foreign currency transactions.

It was noticeable that they had some innovative services which had been designed to get around the restrictions placed on them by law. These services were in line with the needs of the communities and some had been designed to get around the limitation of their catchment area. One of these services is an arrangement that allows people living in cities and other localities to open accounts with the rural banks. This scheme is known as "*efie ne fie"* or as home cash. The arrangement is such that the prospective customers, usually city dwellers, open their accounts from a bank in their locality. This means that ID checks and all form filing are done in the nominated bank different from where the rural bank operates. The documentation is then forwarded to the rural bank to open the account.

They also offer a local money transfer scheme called the apex link money transfer for customers who want to send money to a person living in a locality outside a bank's catchment area. Payment to the recipient of such a transfer is through a different named rural bank which operates in the area.

Aside these services, they also offer other specialised services in line with their clientele's needs. Some of these services include hire purchase/consumer credit arrangements for items like agricultural input items for their customers who are mostly farmers. Another such service they offer is a short loan known as the funeral loan. These loans are for a period of two weeks. In Ghana, funerals are elaborate events usually held at the deceased's home village (Utley, 2009). They are very expensive especially because families have to host guests or relatives who sometimes come from all round the country. However at the funeral ceremony the community make donations

to the family of the deceased. This means that most families end up recovering the initial cost of the funeral. Rural banks therefore offer short loans to cover the initial cost of the funeral which the families are able to repay after the funeral.

Rural banks offer about 14 services in total. Out if these services seven cannot be provided without the involvement of other rural banks, the Apex bank or retailers (See figure 6.1 & 6.2). Most of this is a direct consequence of restrictions to the services rural banks can offer. The implication of this is that business processes for delivering these services start in one bank and end up in another bank or retailer. This creates a complex distributed work process in which no single rural bank has end to end management or authority thus making risk and security assessment and management very difficult. Questions regarding which bank are responsible for identity verification, creation and accreditation are immediately raised.

Figure 6.1: Services Involving More Than One Organisation

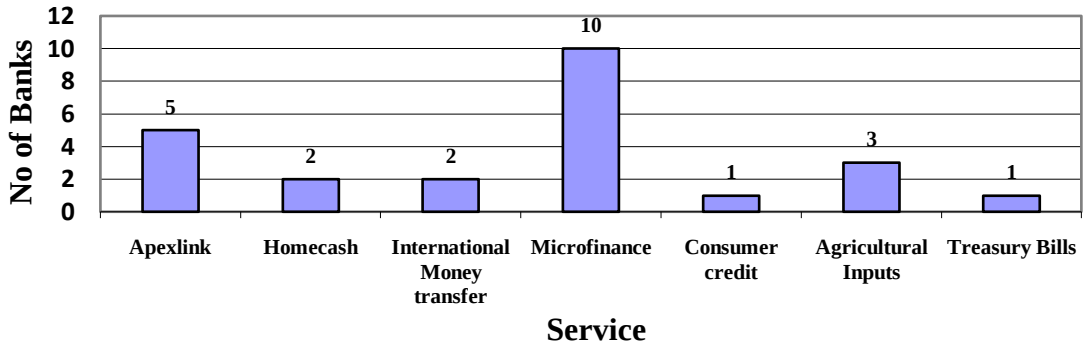
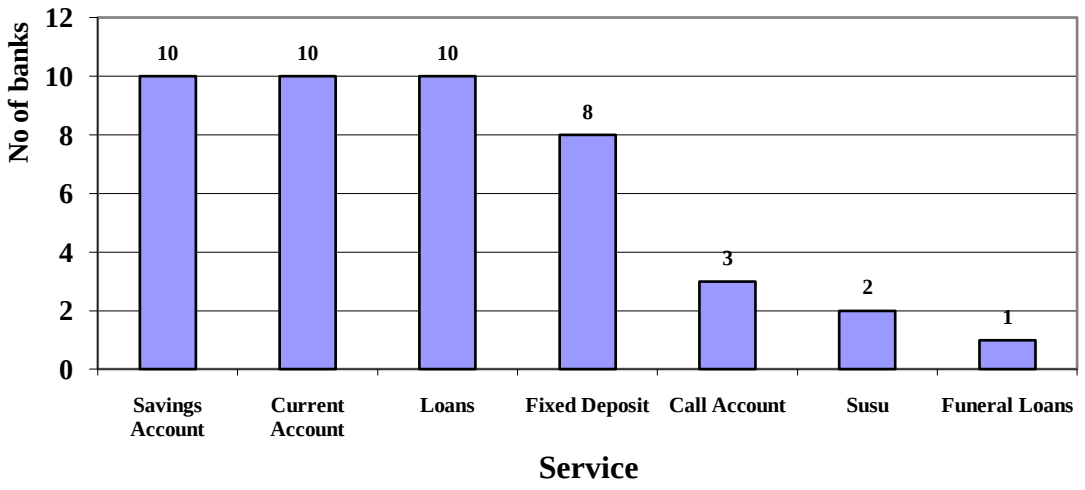


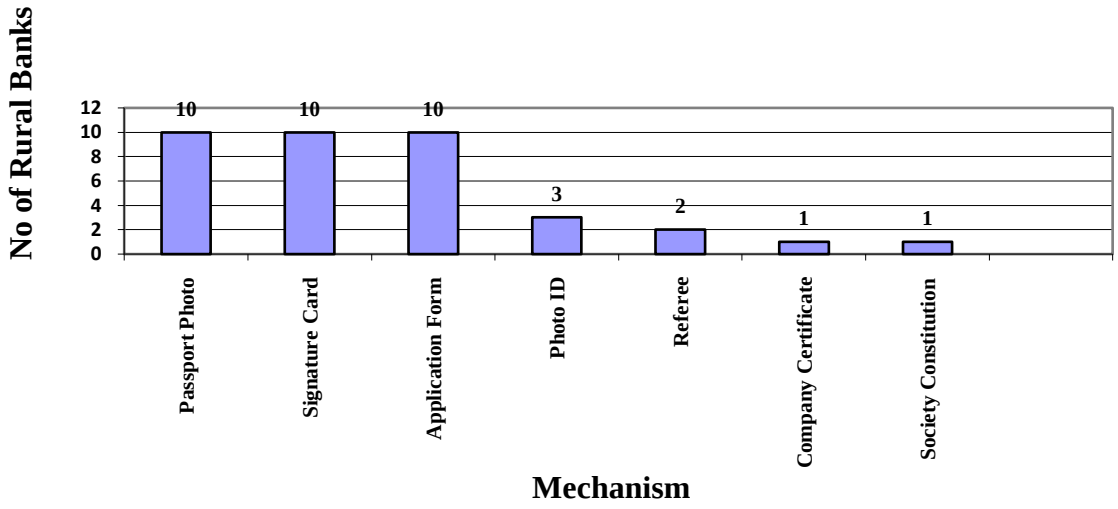
Figure 6.2: Services with No Outside Control



6.2 Customer Identification in Rural Communities

It was evident that rural banks attempt to verify identities of their prospective customers however there was enough evidence that these mechanisms could not do the job. The various mechanisms used are shown in figure 6.3.

Figure 6.3: Customer Identification Mechanisms



The field study revealed that the requirements for creating an identity for the purpose of opening an account in rural banks are a passport sized photograph, a filled application form and a sample of the customer's signature on a signature card. Information filled on the application form with name, address, occupation, employer (if employed) and salary. Two rural banks said they went a bit further to demand a referee whilst three banks demanded some form of photo identification like voter's identity card or driver's license. For corporate bodies one bank demanded company certificate and for associations they demanded the society's constitution. These identity verification requirements seem inadequate to confirm that the personal identification information presented belongs to the person presenting it and that it is correct. It only confirms to the bank employee what the prospective customer has already said.

On the other hand implementation of western style identity checks recommended by the Basel committee does not seem feasible. This is because the underlying structures on which they are based are not present either due to the nature of rural communities or the ease of obtaining these documents. Western style customer due diligence requires

the validation of the provided address, birth certificates, occupation and nationality among others as proof of identity. See chapter 2. The essence of an address for instance is to be able to trace customers to that address. European banks usually require the submission of some form of correspondence from a reputable organisation like a utility company to proof ones address.

As was found during the field study, banks in rural Ghana are unable to ask prospective customers to submit a document to show an address for a hut in a small village because they do not have recognised fixed addresses. This is because there are no named streets or house numbers hence most people cannot tie a document to their address. Even in relatively bigger villages or towns where some streets may be named, the living arrangement of a majority of the people is such that they do not have bills in their names or are from the informal sector of the of the economy so do not have payslips etc. Also in Ghana mail is routed through post office boxes hence a large number of mails cannot be linked to specific landed addresses. Bank employees mentioned that many prospective customers do not have a birth certificate mainly because a good number of them were born at home. As a matter of fact there is no proof that most of these rural dwellers are Ghanaian citizens. On the other extreme were people who have acquired multiple identities especially in the urban areas. Members of staff in the commercial banks spoken to admitted the existence of customers with more than one account which had different dates of birth for each account belonging to the same person. Enquiries at the Vehicle Examination and Licensing Division, the statutory body that issues drivers licenses and the electoral commission revealed that licenses and voters ID cards are issued without verifying the identities. Another enquiry to the registry of births and deaths also revealed that no proof of identity or evidence of a birth is required before a birth certificate is issued. This indicated the ease in getting

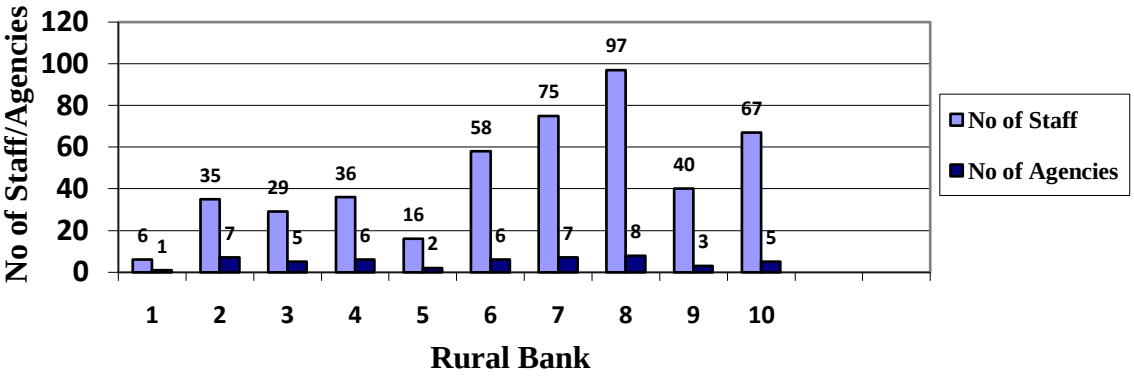
identity documents which seems to be confirmed by several arrests and prosecution of people who had obtained more than one voters ID card in the 2008 elections (Ghanaian Times, 2008 , Ghana News Agency, 2008). The conclusion is that identity verification is weak and that conventional mechanisms cannot work.

Some employees had however devised various ways to verify the identity of customers. A teller in the rural bank mentioned that when third party customers bring in cheques to withdraw money from another person's account they sometimes ask for them to verify their identity by seeking a reference from someone in the community the bank could trust. The person usually fallen on to give such an undertaken is the customer's priest. This is however not a requirement in the bank it is only used by staff members to cover themselves against culpability.

6.3 Staffing levels and its Implication on Security

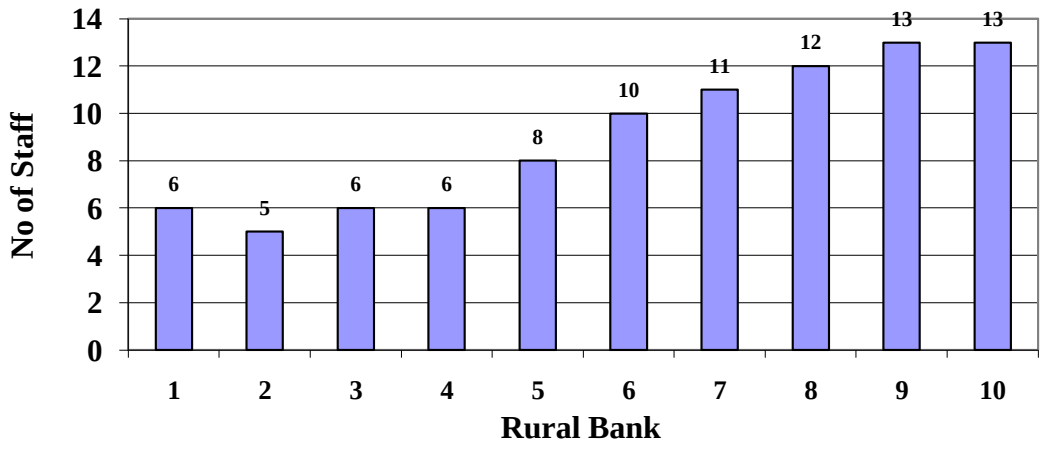
Field studies among rural banks also showed various staffing per bank of rural banks ranging from 6 to 97 per bank. These numbers were distributed amongst various agencies. Figure 6.4 shows the total number of staff and the number of agencies over which the staff are distributed.

Figure 6.4: Total No. of Staff and the No. of Agencies of Rural Banks



There were a total of 459 employees within the 10 rural banks studied. These employees are distributed amongst 50 rural bank agencies and head offices giving an average of 9 members of staff per agency. However not all of these were operational staff. They included administrative and other roles like security. Also members of staff at the head offices were not directly involved in banking operations. Staff members who are therefore available and assigned to carry out banking operations were lower. Figure 6.5 shows average staff per bank for the 10 banks surveyed.

Figure 6.5: Average Number of Staff per Agency



One notable risk which is a direct result of operating with small staff numbers is that separation of duty cannot be effectively achieved given the number of services offered. With an average of 9 employees in total per branch there is an average 4 clerical level staff (2 tellers and 2 general clerks) or less left to initiate and execute the various transactions. There is therefore little room for achieving any meaningful level of separation of duty especially with as many as 14 products/services on offer. The risk of allocating potentially conflicting or risky tasks to the same clerk is particularly high. As was pointed out by a former rural bank employee, this situation is exacerbated by the fact that some of the staff of the banks could be from the same family reducing further the options for separating duties. This former employee mentioned a case where an employee of his former bank continuously cleared the banks suspense account in anticipation of auditors. He even admitted having given unauthorised loans to friends in anticipation of their salary. Though the management of the banks recognised the security risk of having members of the same family working together, they did not admit they had the problem. Rather they mentioned that it is a problem in other banks.

This therefore raises the need to devise other non conventional mechanisms to achieve an acceptable level of separation of duty and to provide an acceptable level of assurance.

6.4 Implications of the Current Organisational Structure of Rural Banks

All the rural banks surveyed had the same organisational structure. A generic structure is shown in figure 6.6. The various positions and their corresponding roles are shown in the table below as shown in table 6.1.

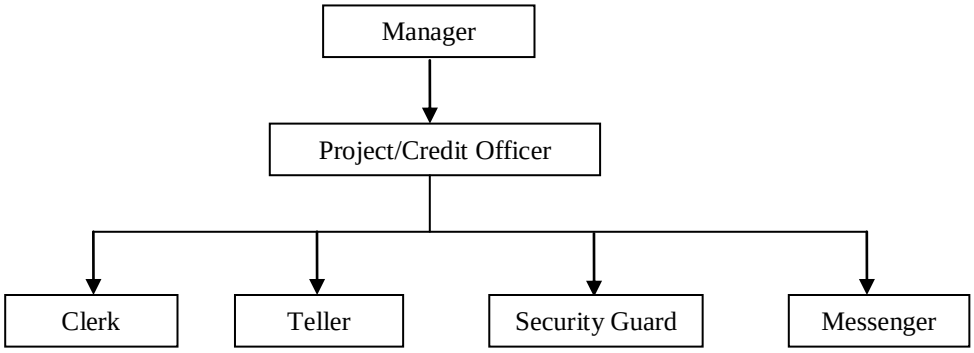


Figure 6.6 Generic Organisational Structure of Rural banks

Job position	Role/duties	Category of duties
Agency manager	General responsibility of managing branch	Approval role
Operations officer	Deals with all day to day operational issues at both the front and back office	Approval role
Project/Credit officer	Appraisal of loans	Initiating and appraising loan applications.
Cashier	Paying and receipt of all transactions	Initiating regarding credit and debit transactions on customer accounts.
Clerks	Filing, opening and closing accounts, posting entries and balancing books, Customer queries and call over	Initiating account opening, closing posting entries and balancing books
Messenger		Non-Banking Role
Security Guard		Non-Banking Role

Table 6.1: Rural banking job positions, roles and category role

Generally banking operations occur at the agency level. The observation which was made and confirmed by the staff was that there are two levels of authority. They are the clerical level and the officer/manager level. Clerical staffs were the ones who initiated transactions at the request of customers or when a banking instruction is received.

Transactions initiated by the clerical staff are then approved by the officer/managerial grade staff usually the operations officer. In most cases the branch manager did not get involved in the daily operational issues rather the operations officer did the approval of transactions unless when there was a case that requires the attention or advice of the manager. The Operations officer therefore has both front and back office control and in turn reports to the branch manager.

According to bankers from the main stream bank, their structure is very different. In the main stream banks there is a customer services manager in charge of the front office and an operations manager in charge of the back office. See figure 6.7

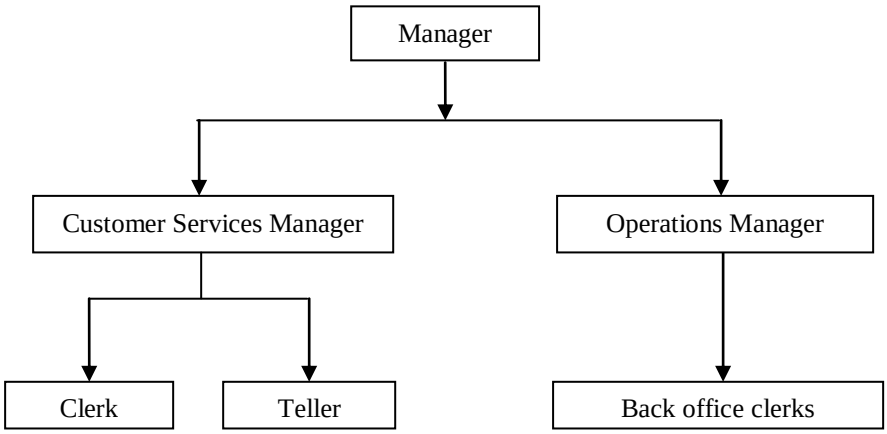


Figure 6.7 Generic Organisational Structure Main Stream Banks

The front office deals directly with customers. They perform transaction like account opening deposits and withdrawals and the back office deals with bank suspense account clearing checks and other interbank and account transfers. The main characteristic of the front office is that a customer has the opportunity to present identification

information and authenticate themselves. On the other hand the back office which deals with transactions without a customer have to use other means to verify authorisation to perform such transactions. They always have to rely on the source document.

A major risk arises as a result of the organisational structure of the rural banks. The risk is due to the control given to managers. The major issue here is that the operations manager who has most of the day to day supervision of transactions had control of the front and back office functions a situation that is found to be risky in financial operations.

When a transaction is performed at the front office there is the presence of a customer with a signed cheque or some form of coded message in the case of the back office for the purpose of authentication. Combining the front and back office under one officer or manager blurs this distinction. The result is that deficient front office transactions can be hidden or passed off as a back office transaction and vice versa.

6.5 Internal Control and Fraud Prevention

The field research indicated internal control measures especially aimed at fraud was solely the responsibility of individual banks. A mixture of control measures were also used however only a few of these measures were targeted at transactions.

Fraud prevention as discussed above is a non prudential regulatory issue and the interview of ARB Apex bank officials indicated that they are not involved in non prudential regulation. The rural banks are therefore left to decide which internal control methods and how they want to use them.

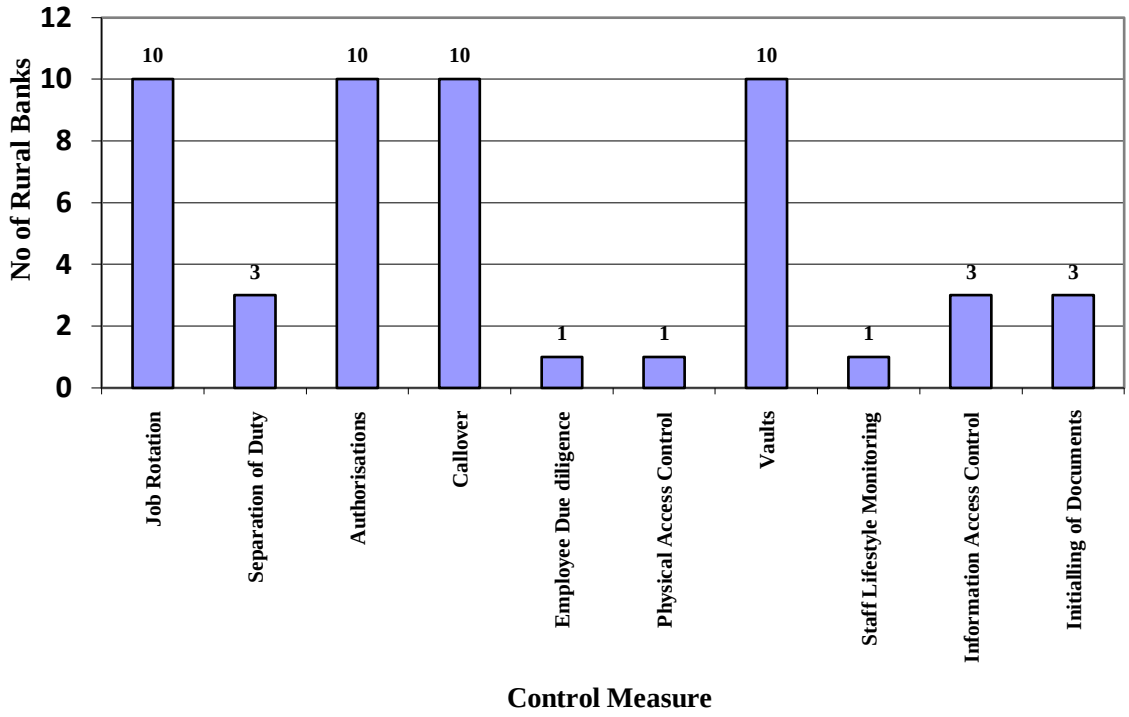
Christen et al (2003) indicates that the two main issues that is of much concerned to non-prudential regulators of microfinance institutions as far as customer protection is concerned are protection against abusive lending and collection practices (lending practices that lead to over borrowing by customers) and providing borrower with truth in lending (accurate comparable and transparent information about the cost of loans). Contrary to this position however, most of the rural bankers spoken to referred to fraud amongst customers and employees as the main threats to their day to day operation.

The field research showed that the rural banks have a number of internal controls measures aimed at fraud control.

One of the most used control mechanism is job rotation but equally used are authorisation of transactions, audit checks (call over) and the use of some physical security mechanisms.

Figure 6.8 shows the internal control mechanisms used by rural banks in Ghana.

Figure 6.8: Internal Control Measures Deployed by Rural Banks

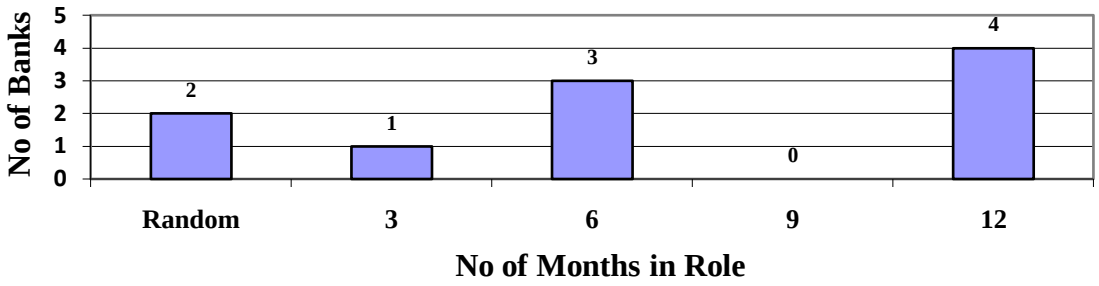


6.5.1 Job Rotation and Security Concerns

Job rotation is one of the key internal control mechanisms rural banks used. This involved the clerical grade employees being assigned different roles for a specified time period.

Figure 6.9 shows the period that members of staff stay in a particular role for the 10 rural banks studied. A majority of 4 banks rotated their staff every year while 2 banks rotated them at random intervals.

Figure 6.9: Frequency of Job Rotation



Job rotation or rotating employees among numerous positions is a known to help organisations improve on security. Aside providing knowledge redundancy it reduces the risk of fraud, data modification, sabotage, theft and misuse of information (Stewart et al., 2005). The view is that when a person stays longer in a position the more likely they are to be assigned more responsibility and gain more privileges and access. They are also more likely to become more familiar with tasks and gain the ability to abuse privileges and commit fraudulent or malicious activities. Job rotation also provides the opportunity for peer auditing and enables employees to detect fraudulent activities of their peers.

Job rotation seems to have benefits however it also presents clear risks in the case of rural banks. The risk here is that employees get the opportunity of performing two unrelated but conflicting tasks that could create opportunity for fraud. This risk is also compounded by the system of deputising for the purpose of filling in for unavailable staff even though these require a manager's approval. Bank staff who know or anticipate what job they would be doing next can do certain preparatory activities in their current job and perform other activities in their next job to complete the fraud. Similar frauds like what occurred in the Société General fraud case could occur. In this case, Jerome Kerviel took advantage of his knowledge of the banks back office and

control systems – a computer system called Eliot – to enter false hedging contracts to make it appear as if he was taking minimal risks (Arnold et al., 2008). He did this by logging into the system under different names, he then cancelled the fake contracts before they were settled, replacing them with new ones. This type of fraud can be replicated if an employee is rotated from position to position especially if the next position is known.

6.5.2 Effectiveness of Authorisations

Rural banks used transaction authorisation as an internal control measure. This means that all members of staff have a maximum amount for which they can perform a transaction without authorisation. Transaction with amounts beyond that of a staff member has to receive authorisation from another member of staff who has a higher limit usually the operations officer or manager. This mechanism is useful by offering a second opportunity to examine large withdrawals. On the other hand authorisation only looks at the amount and the bank officials admitted it's deficiency in dealing with false identity and deceptive mechanism used to perpetrate fraudulent schemes.

6.5.3 Effectiveness of Call over

Call over is another internal control measure is used by rural banks to detect fraud but it also has some defects. This measure involves a daily cross check of recorded transactions against their source documents. This measure is practiced by most rural banks. It was thought to be very effective in detecting fraud and errors by the banking staff. The problem with this approach is that it is a post transaction audit process hence if a fraudster has left the banking premises then there is a huge problem to apprehend the perpetrator. On the other hand since it is a manual process and therefore depends on

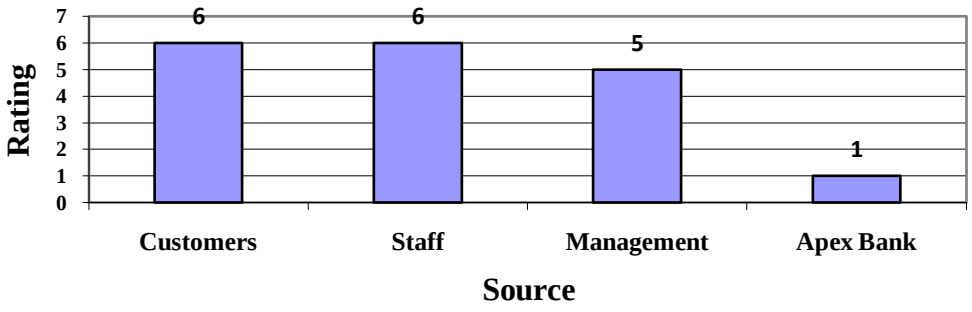
the ability of the staff in question to be vigilant. After working a long day it is easy for tired staff members to miss discrepancies.

6.6 Role of the Various Stakeholders in Fraud

Banking institutions have traditionally been very secretive especially when it has to do with revealing activities that might impact public confidence. They are therefore very wary of reporting fraud. At the least, banks attribute fraud to customers.

Banking institutions are usually reluctant to report on failures in internal controls especially when it leads to losses (Blakley et al., 2001). It is not therefore unexpected that rural banks do not seem to have any fraud reports. Banking staff were asked during the field study to rate the various stakeholders role in non adherence to banking procedures which could lead to fraud. See Figure 6.10.

Fig 6.10: Source of Non-Adherence to proceedure



The result revealed that the two main saboteurs of banking processes were the customers and the staff. It is significant that whilst the bankers admitted their complacency in perpetrating fraud they contradict literature which sees the insider as

the main threat to business systems. The implication however is that with customers and staff forming the weakest link, remedial solutions should be targeted at them.

ARB Apex bank was however largely seen as the least problematic. Interviews with managers of rural banks and a regional manager of ARB Apex Bank revealed that rural banks are autonomous organisations. They are therefore not under any form of direct control from the Apex bank; they are manage themselves the way they see fit. In that regard the Apex bank does not concern itself with the fraud within individual rural banks. The ARB Apex bank is only interested in the possibility of fraud regarding transactions they are processing at their end.

With regards to regulation, the ARB Apex bank is only involved in prudential regulation thus conducting banking inspection on behalf of the Bank of Ghana. They are not involved in non- prudential regulation and for that matter fraud prevention within rural banks.

The ARB Apex bank in several respects operates like a commercial bank for the rural banks maintain accounts and offering services for them. In addition they provide various non banking services. The banking services provided include:

- Specie services which involve physically transporting cash to and from Bank of Ghana.
- Clearing services; between rural banks on one hand and between rural banks and commercial banks on the other hand.
- Apexlink local money transfer. In this type of transaction Apex bank does clearing between the paying and the receiving bank's account. After verifying

that all the transaction details received from the paying and the receiving banks are correct they effect a transfer between the account of the two banks

- *Efie ne fie* (Home cash) which enables account opening and operation from a different locality
- Placid and Surichange International money transfer – the ARB Apex bank serves as the last leg of international transfers receiving inward transfers and passing it on to rural banks

Non banking services provided by ARB Apex bank include;

- Treasury and management advice
- Training and capacity building
- Product development and introduction to rural banks
- There are plans to let the Apex bank take over completely the function of prudential regulation of rural banks. Currently the bank of Ghana does the inspection of the rural banks however the LI1825 mandates the apex bank to do inspections which they are going to carry out in due course.

Though Apex bank is not involved in fraud control within individual banks it can play a crucial role in any security system to protect the integrity of transactions. Due to restrictions placed on the operations of rural banks the ARB Apex bank serves as a link between rural banks. The most important role the ARB Apex bank can play in securing transactions of rural bans is to serve as a platform for implementing mechanisms for transactions that cover more than one bank.

Currently it directly participates in transactions involving more than one bank. Due to this role it has access to all rural banks hence it could serve as a repository of

information and knowledge relevant to fraud prevention unlike individual rural banks. Information such as risky customers or employees could be shared with rural banks. It could also serve as a secure means of transmitting transfer information between rural banks. Currently rural banks have to call each other on the phone to relay transfer information. ARB Apex bank could also serve as a means of reconciling information about transactions which cross organisational boundaries to prevent fraud.

6.7 Summary of Systemic Weaknesses

Several systemic weaknesses were identified during the field study. These weaknesses were mainly due to two main causes. The first is the regulatory regime that the rural banking system operates under. The second is the nature of the rural communities the banking system operates in. There were many structural and soft issues within the community that made some conventional banking practices inadequate.

Half of the services offered by rural banks have business processes that cross organisational boundaries. This increases the vulnerability of the process and increases the risk of fraud since you have more than one entity being responsible for ensuring security.

It was also observed that rural banks have small staff sizes. Small staff sizes reduce the ability to effectively implement separation of duty. The ability to deal with fraud is therefore reduced.

Others involved non existence of structures and mechanisms to properly identity prospective customers. Also identification documents available are not reliable to be used for effective identity verification.

Other internal control mechanisms like job rotation, call over and authorising transaction were used to prevent fraud. These were thought to be inadequate in dealing with the risks. Staff and Customers were thought to undermine the implementation of some of the banking processes including internal control mechanism. Any new control mechanism should therefore be aimed at these two main groups of people who from the weakest link.

The ARB Apex bank is not involved in fraud prevention however they were involved in a number of transactions and had access to all rural banks. This puts them in a position where they could serve as a platform for implementing measures to control fraud.

The next chapter looks at the manifestation of these systemic weaknesses in banking processes. In other words what possibilities exist for example a criminal if they could obtain two drivers license and if the banks rely on a driver's licenses to create customer identities in the account opening process.

Chapter 7

7 Rural Banking Processes and Fraud Risks

This chapter is primary aimed at presenting how fraud can be manifest within the banking processes. First it looks at the flow of money within the rural banking industry as a target for fraudsters. It starts by looking at accounts as the main vehicle for banking it also does a general discussion of in account transactions and the risks associated. There is also discussion of source documents, loans, the importance of customer static data and the risks associated with it.

There is subsequently a presentation of twenty fraud scenarios that illustrate the manifestation of fraud in the banking processes. These scenarios are instances of fraud that have occurred in the past or cases that could occur as a result of systemic weaknesses that were found during the field research. They were created with the help of rural and commercial bankers.

Finally there is a discussion of the issues that give opportunity to commit fraud in rural banking. This discussion leads to requirements for a fraud control.

7.1 Flow of Money within the Rural Banking Industry

Fraud occurs when the flow of money represented by transactions targeted in such a way that unauthorised people benefit. Figure 7.1 shows the rural banking system and the flow of money around the system. The diagram shows three main types of entities. They are the customer, the rural bank suspense account and the customer account. It is worth noting that bank employees are involved in all transfers. These are the main points through which money flow in rural banking. ARB Apex bank is also represented as a participant when money flows between two banks. The arrows show the flow of money around the system which occurs during transactions. It also shows flow of money between accounts which does not involve cash.

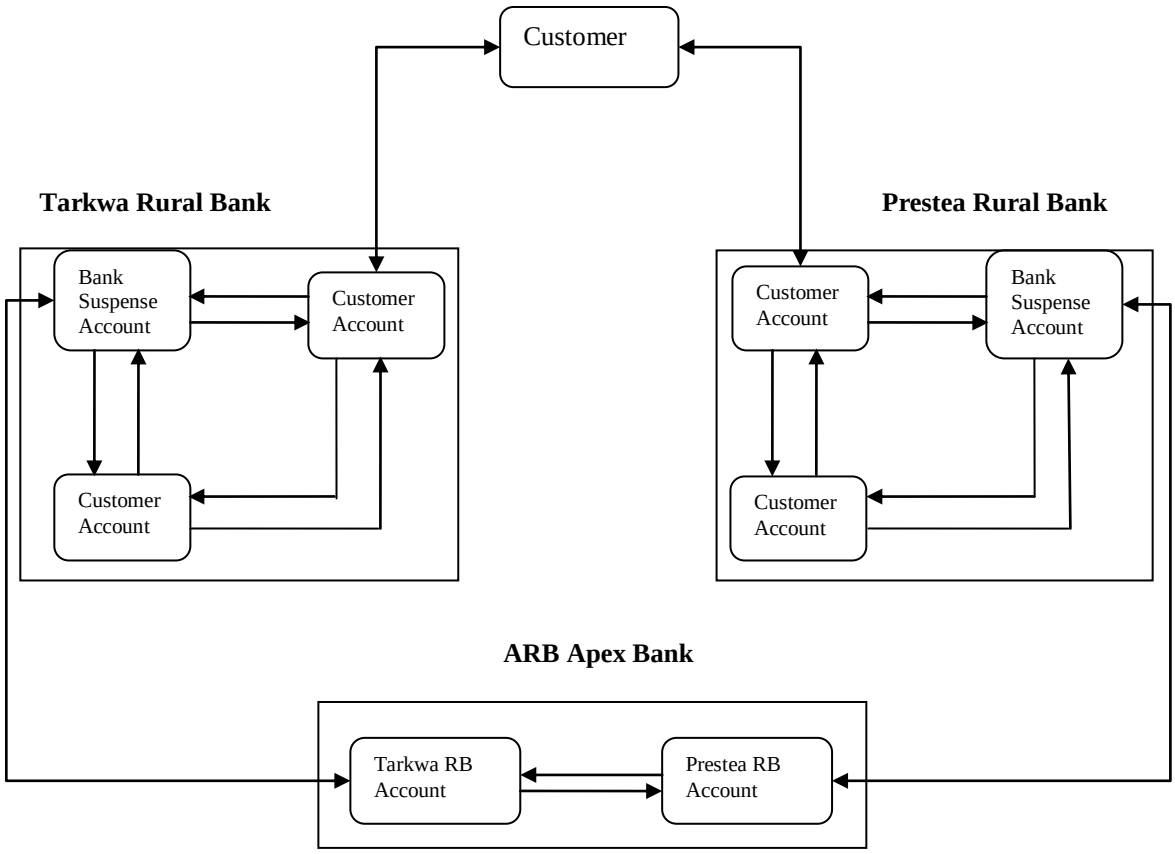


Figure 7.1 Rural Banking Process and Flow of Money

Where the transaction is within a rural bank it involves employees of that bank. On the other hand if it occurs in the ARB Apex bank then it involves apex bank staff. When a transaction occurs between two organisations the part that occurs in an organisation is dealt with by its staff. Details of the banking processes are in appendix C. A detailed discussion of how this fraud occurs is discussed shortly.

7.2 Bank Account and Account Transactions

The basic banking service in rural banking is the customer account which could be in the name of an individual or organisation. Accounts are created to record monies owed by the bank to a customer or the customer to the bank (in the case of a loan) and it has a record of all transactions performed by a customer. They are therefore opened in the name of a specified customer(s) who might be an individual or a company. Hence customer identity is closely linked to the opening or creation of an account. It is this individual that the bank assumes they are doing business with. It is therefore critical that the identity of the person who requests a transaction on an account be thoroughly verified.

There are various types of customer accounts in rural banking but the two most common are the savings and current account. Rural banks offer current accounts which usually come with a cheque book which serves as a means for withdrawing money from the account and for making payment to another person. They also offer savings accounts that pay interest on deposits but do not offer a cheque book and so cannot be used to make payments like a current account. These accounts usually have a credit or positive balance which means the customer has money deposited in the bank. A customer account can occasionally have a debit balance when an overdraft facility is granted and used in such a case the customer will owe the bank.

For the purpose of discussing scenarios customer accounts have been grouped into one because they basically have similar account opening processes which have been described in the preceding chapter.

Rural banks also open various accounts to enable their operations. The suspense account is one of such account. These are used for funds receipts that are doubtful or may have discrepancies pending resolution and subsequent disbursements. When accounts do not balance the excess money is usually placed in a suspense account. They are also used when funds belong to a person who does not have an account in the bank usually referred to as money in transit. They are also used to hold monies in transit like in the Apex money transfers. Generally suspense accounts are meant to be zero balance account (O'Gara, 2004) and bankers from both the main stream and rural banks confirmed this. When there is a balance on a suspense account the indication is that some funds have not gotten to its destination account or money has gone out of the bank which needs to be in the bank. The implication is that all discrepancies must be resolved. During the field study, suspense accounts were said by the bankers to be one of the targets of inside fraudsters. Access to and use of Suspense accounts, they said, must be tightly regulated to ensure that they are used for the purpose for which they have been created and accessed by only those who are authorised to do so.

All banking processes involve transactions on an account. Account transactions are either a credit transaction or a debit transaction which would deposit or withdraw money from an account respectively. In an account transfer transaction for example, there is a debit transaction and a credit transaction taking money from one account and depositing it in another. The various account transactions are described in Appendix C. Being the main focus of transactions, insertion, deletion or modification of a record in

an account gives legitimacy to a transaction at least on the surface. It is therefore critical to prevent fraudsters from assuming the identity of a legitimate customer to enable a transaction to be performed on an account. It is equally critical to prevent rogue staff from illegally amending records of an account to enable them to take money from the bank. On the other hand it is important for a bank to have the ability to prevent a customer from denying that a transaction was authorised by them. One such abuse which employees were said to have used to commit fraud in the past was reversing transactions. Employees are allowed to reverse a transaction which has already been processed if there is a mistake or some problem with it. They were however said to have in the past reversed the transactions to have access to the monies involved.

Another risk occurs in cross organisational transactions like the Apexlink money transfer. This service enables customers to transfer money from a bank in one locality to another person through another bank in another locality. This is in essence a series of account transfers but it also includes various mechanisms for clearing and the proper identification of the recipient. With neither of the banks having end to end management of the whole process and therefore fraudster could insert amendments to the transaction for their benefit. With recipients of these transfers are not required to be customers of the paying bank therefore it increases the risk of the money ending up in the wrong hands. This is because banks pay money to non customers based on the identification provided by the recipient hence if the ID provided is fictitious there will not be a mechanism to trace them.

7.3 Cheques and Source Documents

Source documents are used to initiate transactions. They are issued internally or issued from a customer. A cheque is an example of a source documents. It is a document that

is used to instruct a bank to pay a specific amount of money from a specified account held by the bank. It is therefore a very sensitive document because when filled and signed it could put money in the hands of a criminal.

The use of forged documents especially cheques to make a fraudulent withdrawal was noted as a problem recently by all the bankers interviewed. An account can fall to the mercy of a criminal given that the account number is known and the customer's signature can be reasonably forged.

Generally a cheque would bear the details of the bank, the drawers name, the account number and the cheques number printed on it. Cheques also have the amount to be drawn both in words and numbers, the signature of the drawer/ customer, the date and the name of the payee.

Though the printed details are printed in machine readable Magnetic Ink Recognition Character (MICR) cheques can be forged when the fraudster has access to the technology. In any case all the banks visited did not have machines to read the cheques anyhow so if they are forged with non machine readable ink it would not have been noticed.

Again the signature of the customer which is usually the main verification mechanism can be forged together with the amount and the date. Access to cheques is therefore seen as critical in fraud prevention.

7.4 Amendment of Customer Static Data

Static data like name, signature, and contact details like address and phone number are kept on account holders when accounts are opened. As in most banking institutions all

over the world, banking customers go through various circumstances that cause them to change their personal identifications information. It is not unusual for customers to change their addresses when they move house, a phone number or even a name during the life of an account. Additional signatories could be added for corporate customers in a case where management changes.

In changing account details customers are asked to bring letters or powers of attorney to prove that the customer has given consent to the bank to change the details. This is to ensure the customer does not deny authorising the change in the future. This request assumes that the letter supplied came from a genuine attorney. In the case where a letter is purported to come from the customer, the assumption that it came from the customer is based on having the letter bearing the customer's signature. This brings into question the reliability of signatures and the ability to detect forged ones. New scanner technology makes forgery easy and undetectable (Deposit Account Fraud Committee, 2000) while criminals can even go further and fraudulently use autopens. Experiments conducted with signature forgers who were new to the task of forging indicated 29.4% were successful forgeries. This was despite the fact that thorough inspection done by people who knew there were forged signatures samples (Cvrcek et al., 2005). This shows that the whole process of human signature identification is at best unreliable.

Changing static data introduces another person or a means for another person to impersonate an account holder. In a case where the fraudulent change is perpetrated by an employee who changes or adds a signatory to an account, the whole mechanism of fraud detection becomes dead from the start because the signatory will subsequently be seen as an authorised party for that account.

7.5 Loan Application

Bank loans involve a bank lending a sum of money to its customer to be repaid at a later date. In giving out loans, banks willingly give out money to customers. It is thought an easy way to take money out of a bank is to take a loan and this is because bankers most often encourage customers to take out loans. Criminals can either use misrepresentation of their financial circumstances or set up fictitious accounts for nonexistent customers to contract a loan.

In the rural banking system the project officer is usually the one who receives and appraise loan applications. Within this process they can easily aid in making a misrepresentation for such an application for a loan. This risk is high when it is combined with the mechanism of job rotation, a project officer who has already set up fictitious accounts could apply for loans for such an account.

Overdrafts are facilities that banks give to their customers to enable them to take more money from their account than they actually have. In other words it could be seen as another form of loan. Generally overdraft facilities in the rural banks are only allowed when there is prior arrangement with the manager. Overdraft which is a form of a loan could be used by criminals to siphon money from a bank especially when the account which is offered the facility is a fraudulent one.

Hire purchase arrangements are also offered by rural banks where the bank finances for example equipment for the customer. These hire purchase arrangements are done to ensure that loans given to customers are used for what they are given for. Loans and hire purchase are also put into the same category because they also follow a similar

process for applying, appraisal and approval irrespective of the amount or whether it is part of a larger government program.

7.6 Fraud Scenarios

As mentioned earlier the fraud scenarios were arrived at based on the frauds which have either occurred or had a high possibility to occur due to systemic weaknesses. They were arrived at after observation, interviews and discussions with various employees of rural banks and other commercial banks.

In presenting the fraud scenarios various fictional characters have been created to discuss possible scenarios that were arrived at during the field work. Three fictitious banking institutions are used to illustrate the fraud scenarios. They are made up of two fictitious rural banks operating in different localities. These are Tarkwa rural bank and then Prestea rural bank. There is also a class 1 main stream bank commercial bank Accra bank.

The scenarios also make use of various fictitious characters. Within Tarkwa rural bank there is Yaw who is an employee has various roles in the bank. Yaw assumes the various positions through job rotation. There is also Ato who is an operations officer of Tarkwa rural bank.

There are also customers within the scenarios. There are Fiifi and Ebo who are both account holders of Tarkwa rural bank. There is also Jojo who is an account holder of Prestea rural bank. Then there is Esi a fraudster who is not a customer of any of the banks. Ama is a fictitious identity used to commit fraud. The last two characters are Kwasi and Yaa who are not account holders.

7.6.1 Fraud Scenario 1 - Unauthorised withdrawal

Yaw a bank employee uses his status as an authorised officer of the bank which allows him to perform transactions. He uses this to perform a fraudulent withdrawal. Yaw performs an unauthorised withdrawal from Ebo's account with the intent of stealing the money. This means that Yaw does the withdrawal without a cheque or internally generated voucher which should act as a source document on which the transaction is initiated. Normally the bank does a call over which is an end of day audit to match all transaction for the day with their documentation. This mechanism is meant to detect all errors or fraud. The risk that could allow this fraud to occur is that if the call over is not done properly or there is an oversight by the call over staff. On the other hand if Yaw decides to leave before the end of the day the fraud would succeed. This is because the mechanism can only detect the fraud at the end of the day when the fraud has been perpetrated. Also in certain cases the work load or absenteeism prevents banks from performing the call over.

Unauthorised withdrawal from an account could be done in two ways:

a. In the first instance the withdrawal from Ebo's account could be transferred by Yaw into Fiifi another customer of the bank's account. A subsequent withdrawal could then be made by Fiifi from his account and given to Yaw this is to avoid a trail leading to him.
b. Alternatively Yaw can just withdraw the money from Ebo's account.

Every transaction must have a source document but it is possible to carry out a transaction without one. It only becomes an issue during audits. The weakness being exploited here is the ability to process transactions without a source document. Some members of staff in the rural banks indicated that this form of fraud was possible in the

rural banking system. This and the next scenario had actually occurred in a commercial bank.

7.6.2 Fraud Scenario 2 - Unauthorised withdrawal/loan

In this scenario Yaw claims to have authorisation to make withdrawals from Ebo's account based on verbal instructions. Here he is not a teller so cannot perform the transaction so requires a document that would enable him to demand that the transaction be performed. Yaw claims the instruction was given by a telephone call from Ebo based in this fictitious claim he generates an internal withdrawal voucher on which a transaction would be based to make a withdrawal. This scenario can have two variations. With this type of fraud the customer's vigilance is the only means by which the fraud can be detected. Customers who go through their statements thoroughly are the only ones who can detect transactions they have not done. A careful choice of a customer can easily deal with this risk of detection. Here Yaw

a. In the first instance Yaw gives the money to Kwasi as a loan. Kwasi who is a not a customer of the bank and needs a loan Kwasi then returns money in a week and Yaw then pays the money back into Ebo's account taking interest on the loan.
b. In the second case Yaw makes the unauthorised withdrawal transaction on Ebo's account as per verbal instruction and an internal voucher, takes the money and does not return the money back to the account.

The weakness being exploited here it the possibility to use deception to gain fraudulent authority of the customer and access to a valid source document under pretence. In one of the rural banks surveyed a case was related where an officer used this mechanism to

withdraw money from a customer account but returned it after using it. With the weaknesses in the call over mechanism the second variation could also occur.

7.6.3 Fraud Scenario 3 - Same day reversal

Yaw working as a teller processes a deposit transaction for Ebo however after the transaction has been processed, he under the pretext that the transaction is a mistake, reverses the transaction before it goes through call over and is validated. In all the rural banks visited, employees need additional authorisation to reverse a transaction if a mistake is detected. In this scenario, Yaw has the authority to perform the transaction but he needs additional authority to reverse so he creates the deception to obtain the authorisation to perform the reversal. It was indicated that when a transaction is processed and is immediately detected to be wrong it is reversed but not as a separate transaction from the original one just a correction. On the other hand, a transaction reversed a day or more later is usually treated as a whole new transaction and would therefore require more rigorous checks. Yaw therefore makes a request for a reversal of Ebo's deposit transaction minutes after Ebo's original transaction. He keeps the money without going through rigorous checks.

This transaction could also be manifest in two ways;

a. When Yaw credits account of Ebo he could reverse the transaction claiming the amount as a mistake. He would then substitute the original pay-in voucher for his fictitious one with a lesser amount and taking the balance of the money in cash.
b. On the other hand Yaw could reverse the transaction taking the money from Ebo's account and then credits it to Fiifi's account. Here Yaw would claim that to be the original transaction basically substituting the original pay-in voucher

with his fictitious one for Fiifi. He would then ask Fiifi to withdraw the money for him at a later date.

Employees could commit fraud by taking advantage of weaknesses in control measures. Here the ease of employees to undo a transaction could be exploited to commit fraud. The bankers in the commercial banks spoken to said it used to be a problem in the past and some of the rural bankers agreed that it could occur in their banks.

7.6.4 Fraud Scenario 4 - Job Rotation Fraud

As discussed in chapter 5, one of the main internal control measures that rural banks use is job rotation. This in itself is a good mechanism however it has a down side which presents fraudsters with an opportunity. In many cases some transactions may not by themselves be risky in terms of direct loss to the bank. They can however create an opportunity to create deception for the purpose of committing another fraudulent transaction. With this fraud type Yaw needs to create a new identity to enable him to request for a loan and also to enable him to avoid being traced hence the need to create the deception with a new identity.

Yaw opens a dummy account for nonexistent customer Ama when he is on rotation as a customer services officer. Now in another capacity Yaw can apply for credit for the fraudulent account. When the said credit has been accessed the nonexistent owner cannot be traced. This fraud can be manifest in 4 ways.

a. Yaw opens a fictitious account in the name of Ama when on rotation as an account opening clerk. Applies for a loan for Ama with forged guarantors when on rotated to the loan desk.

b. Yaw opens a fictitious account in the name of Ama when on rotation as an account opening clerk. Request for an overdraft and spends the money without paying

c. Yaw opens a fictitious account in the name of Ebo in his bank Tarkwa rural bank in the same name as an existing customer Ebo when on rotation as an account opening clerk. Yaw then opens another fictitious account in Prestea rural bank in the name of Ama. Yaw would then pay a cheque belonging to the real Ebo into the false account when he is on rotation as a teller. He can then write a cheque for the fictitious Ebo account to be paid into the fictitious account in Prestea rural bank in the name of the fictitious customer Ama. When the transfer is made Yaw can then withdraw the money from the Prestea rural bank account in the name of Ama.

d. Opens a dummy account in his bank for a non existing customer with the same name as Ebo when on rotation as an account opening clerk. Yaw would then pay a cheque belonging to Ebo in to the false account when he is on rotation as a teller and withdraw the money.

Here again flaws in control measures are shown to enable an employee to commit fraud. There is no means for a rural bank to determine whether the actions of an employee in one role will enable him to commit a fraud in another. By getting the opportunity to work in different job roles an employee can learn the weaknesses in control measures create deception like fictitious account and also cover fraud. This type of fraud has occurred in many banks across the world the Donald McKenzie case in the Royal bank of Scotland and the Jerome Kiervel Société General case. It was agreed that there was a distinct possibility that this could also occur in the rural banking industry.

7.6.5 Fraud Scenario 5 - False cheque book request

Yaw request for a new cheque book for Ebo with a forged cheque book request slip. To make a withdrawal there needs to be a valid cheque hence Yaw needs to be able to obtain that document that will allow him to create that deception that a withdrawal request is coming from the account holder. When Yaw is working as a customer service officer it is much easier to use a forged cheque request than a forged cheque because he is the one that has to verify it. He therefore takes the cheque book when it arrives at the branch, forges Ebo's signature to make a withdrawal.

This type of fraud has two main variations where

a. Yaw can make a cash withdrawal from Ebo's account using the cheque with a forged signature.
b. On the other hand Yaw could also make a withdrawal from Ebo's account by paying a cheque into Fiifi's account. A withdrawal is then made by Fiifi and the money handed to Yaw.

Forgery is used in this scenario to create a document that enables the fraudster cause deception to enable a fraud to be committed. The weakness in the rural banking system that makes this fraud possible is that there is no reliable way of verification of source documents except by their print design which can easily be replicated by current technology. This scenario was arrived at observing bank officials receiving new cheque book requests. It was observed that cheque requests was not keenly scrutinised like cheque withdrawals.

7.6.6 Fraud Scenario 6 - Signatory alteration

Yaw on rotation as a customer service clerk can add a signatory to Ebo's account. A signature is required to make a withdrawal so when Yaw is working as a customer

service clerk he adds a signatory to Ebo's account details. Here again Yaw chooses to add the signature because that is where he has control and is able to create the deception without being discovered. When he goes on rotation as a customer service person he could then use his access to a counter check as a customer service officer make a withdrawal. Counter cheques are cheque leaflets that are given to customers to use when they do not bring their cheque books to the bank.

Here again this fraud scenario shows that in some roles, an employee in a bank can create documents and records that can enable the commission of fraud without proper controls to prevent abuse. Yaw is therefore able to create such records and documents to support his deception which enables him to commit the fraud. This scenario was also arrived at after observing the lack of mechanisms to detect false request and the poor scrutiny and lack of dual checks to request to change customer static data.

7.6.7 Fraud Scenario 7 – Local Money transfer

Yaw transfers money on behalf of Ebo to Ama who is at Prestea a different locality from Tarkwa and has no bank account. The local money transfer is therefore from Ebo through Tarkwa rural bank to Ama through Prestea rural bank. Ama is therefore required to collect the money in cash. Yaw however passes the transfer details to Esi before Ama claims the cash. Esi then presents herself as Ama before Esi turns up and collects the Money.

Here the inability to match identification information to a natural could result in a fraud. Normally a photo ID is requested and this could be a voter's ID card. A Ghanaian voters ID does not have any security features besides there has been many reported instances of multiple voter registration with different names. Also with the

creation and transmission of identification information to be used by Ama in collecting is left to one person then the risks increases. This enables impersonation of Ama by Esi.

7.6.8 Fraud Scenario 8 - Account opening

Yaw opens a new account in Tarkwa for Fiifi who lives in Prestea. He collects Fiifi's initial deposit to pay into the new account when it has been activated. He however does not pay the cash into the account. This type of fraud, the bankers mentioned, is especially possible when the customer does not live in the same town or even abroad. In such a case Fiifi will not be able to detect whether his deposit was paid into the account or not. This type of fraud is possible because Fiifi being a new customer is not conversant with the normal paying in processes and would accept any instruction given by Yaw who opened the account especially when he trusted him. Though a pay in receipt is given to Fiifi it is only a stamped customer copy of what Fiifi filled in and not one printed of the system as a result of a transaction. Fiifi is unlikely to confirm whether all has been made to the account until the next time he comes to town which could sometimes be up to a year.

There are two variations to this type of fraud

a. When Yaw never pays the money into Fiifi's account
b. When Yaw uses the money for a short term interest activity like a loan to Kwasi and pays the money back.

In this fraud scenario Yaw builds trust in such a way that Fiifi accepts his offer to pay in the cash for him. It also occurs because paying in an initial deposit is a separate transaction as the account opening process though a minimum deposit is required for every account opened. This fraud had occurred in one of the rural banks studied.

7.6.9 Fraud Scenario 9 - Systems admin log in fraud

Some systems administrators have access to log in information or sometimes have the right to override employees when there is a problem with the computer system or if some system functions have to be run like some end of day reports. Yaw working as a systems administrator uses his access to employee login profiles to take Ato's login details. Yaw fabricates a transaction as if it is has been performed by Ato. Transfers money from Ebo's account into Fiifi's another Fiifi collects the money and hands it over to Yaw.

The weakness here is the poor implementation of separation of duties which allows some system administrators to have access to some security information. Ato though a systems administrator cannot perform customer account transaction with his own set of permissions. He therefore needs to create a transaction that is seemingly coming from Ato for it to look genuine. This fraud was committed by an employee of one commercial banks several times before it was discovered.

7.6.10 Fraud Scenario 10 - Dividend payment

For customers who have made investments like shares, dividends from those investments are paid directly into their bank accounts. Ebo's dividend is sent to Tarkwa rural bank by ABC Ltd in which he has invested. These payments come in bulk to the bank with a list of all investors who have accounts in Tarkwa rural bank. Disbursements are then done at Tarkwa rural bank. Yaw therefore pays the bulk amount into the bank's suspense account. In making the disbursements to the various investors Yaw pays Ebo's part of the money into Fiifi's account. Fiifi then withdraws the money and gives it to Yaw.

The weakness that is exploited in this fraud is that bulk inward transfers are not automatically credited to specific accounts. In that case it allows staff members to be able to vary the destination account without the consent of the payee. This is the same for cheques paid in by individual and companies. It is the staff members who manually enter the account details they could enter it into a wrong account without detection. The specific risk with inward transfers is that the recipient does not always know transfers are coming in and hence might take time to detect the fraud. This fraud was committed by an employee of a commercial bank and the rural bankers confirmed that it is a possibility.

7.6.11 Fraud Scenario 11 - Suspense account

In this scenario, an inward transfer to Ebo has mistakes and so cannot be credited to Ebo or any other person for that matter as the details do not match. With the inconsistencies in the transaction the money stays in the suspense account. Yaw debits the suspense account to takes the money

a. With an unclaimed transfer meant for Ebo who is an account holder sitting in the suspense account which is required by regulation to have a zero balance. Yaw takes the opportunity to debit the account and takes the money in cash purporting to have found the rightful recipient.
b. With Ebo an account holder's transfer in the suspense account, Yaw transfers the money into Fiifi's account claiming him to be the rightful owner. Fiifi then withdraws the money and gives it to Yaw.
c. In this variation an unclaimed inward transfer meant for Ama who is not an account holding customer. Yaw passes on the details for Esi to claim the money purporting to be the rightful beneficiary.

d. Also with an unclaimed inward transfer is to Ama a non customer in the suspense account. Yaw transfers the money into Fiifi's account. Fiifi withdraws the money and gives it to Yaw.

Suspense accounts are known to be an immense source of fraud in many organisations (O'Gara, 2004). This is mostly due to the fact that they are designed to contain items of questionable origin destination or in transit. There is therefore the tendency to use any means to try to reduce the balance to zero. The question is whether the destination accounts or recipient is the rightful one. Staff from the rural banks indicated that the weakness is that time limits for balancing these accounts are not adhered to. Also because of the inability of to tie transfer information to an identity of a natural person or an account deception and impersonation becomes possible. Numerous examples of this fraud type were described by bankers from both the rural and commercial banks.

7.6.12 Fraud Scenario 12 – Teller till fraud

Yaw working as a teller at the end of a working day is allowed to keep a small amount of money in his till at the close of the day and the locked till kept in the strongroom. This money is the notes and coins that do not form a round sum. Yaw uses this money which should have been kept in the till to give small loan to Kwasi to make a profit. Yaw returns the money when Kwasi returns the money.

The weakness is that physical cash is difficult to match to electronic money on computer system. It might show that money is in the till or in the strongroom but in reality the money might not be there. A Teller from the rural bank admitted having borrowed money from their till for personal use and returning it at a later date.

7.6.13 Fraud Scenario 13 – check Kitting

Cheque kitting could be a major problem in situations where a reliable system of verifying whether cheques from other banks are not bad cheques. The current method is to wait for a set number of days usually three days before the cheque is given value. This does not necessarily mean that the cheque would have gone through clearing and verified to be good.

In this scenario Fiifi deposits a bad cheque to Prestea rural bank cheque for a large amount issued by JoJo into his Tarkwa rural bank account. Meanwhile Fiifi has already issued a cheque to Ama to withdraw an amount. He then convinces Ato the operations manager to pay Ama's cheque with a smaller face value because a larger amount is coming into his account. He takes the money from Ama and uses it for his purpose. By the third day or more the Prestea cheque issued by Jojo would be found to be false but Fiifi would have taken out the money from the bank or even ready to return it after using it.

Here Fiifi gains the trust of Ato to cause him to grant payment based on the belief that the cheque will be cleared and the amount will be covered. This is partly a trust based fraud. This fraud scenario obtained from two cases one of them involving a sum of about $720,000 and several cheques over several years.

7.6.14 Fraud Scenario 14 - Account opening with false ID

Banks are set up to serve customers and it is paramount that customers are who they say they are. This is because when money is paid into customer accounts or when loans are granted, it is assumed that the bank is doing business which someone who is traceable. An account opening fraud occurs in the various forms. Esi opens an account with fraudulent identity information. Rural banks require just a passport photo to open

an account. Only a few rural banks require a photo ID for identification as discussed in the previous chapter.

a. Esi forges a Ghanaian voter's ID card in the name of Ama. The voters ID card is just a laminated card with no security features. She uses this card to open a bank account at Tarkwa rural bank. She then applies for a loan on the account which has the name Ama on it with the intention of not paying it.
b. Esi obtains a new birth certificate in the name of Ama without proving she is the one (see chapter 5). With a forged birth certificate she can obtain any other document like a passport which she can use to as proof of identity to open an account with Tarkwa rural bank. She then applies for a loan on the account which has the name Ama on it with the intention of not paying it.
c. Esi opens an account with Tarkwa rural bank with her own ID documents but gives a wrong address. She then applies for a loan on the account then disappears. With the wrong address she cannot be traced.

This is a classic case of identity fraud. As discussed before identity information is used for the purpose of distinguishing a person from another it should also be able to help a business trace the person whose identity it is. Giving any form of wrong identity information is to create deception to gain a status which will accrue certain benefits or to avoid being traced when the need arises. Almost all the bankers spoken to mentioned at least one case of identity theft. There were also some of these cases also reported in the news especially in during the electoral commissions 2007 registration exercise.

7.6.15 Fraud Scenario 15 – Employee hiding true ID

In this scenario Yaw seeks employment with a false identity. Three variations of this fraud type were envisaged.

a. Yaw obtains a forged certificate and a birth certificate and passport to create a fictitious identity. He then uses the new fraudulent identity and qualification to seek employment to enable him gain access to the banking system as part of an organised crime syndicate.
b. Yaw in applying for a job uses a different address and refuses to declare his correct address and other important personal information like employment history to create a deception. This deception is to avoid being traced if the need arises.
c. This variation similar to the first one but has a different motivation. Here Yaw obtains a fictitious identity and refuses to declare past history to hide his dubious past. Yaw obtains a forged certificate and a birth certificate and passport to create a new identity. He then uses the new fraudulent identity and qualification to seek seeks employment

There is a risk that prospective employees may want to hide their identity or their history of fraud. A fraudster might also want to seek employment with a different identity for the purpose of committing fraud because it is easier for an employee to commit fraud since they are closer to the banks systems and have more access. Such fraudsters could do so to help them get a job and to avoid being traced in the event of a fraud. This scenario was partly related to the previous fraud scenario when perpetrators used various levels of fraudulent identity.

This fraud is mainly possible because of the difficulty of matching the natural person to the identity identifiable information and the ease of obtaining identity documents. One of the rural bank managers interviewed mentioned that the one of the things they look

at was the character of the employees. He however admitted that it could be a problem if the employee used a false identity.

Fraudulent withdrawal

As discussed earlier cheques are a major means by which customers authorise withdrawals from their account. Cheques can also be used for payment and therefore are sometimes issued by customers to third parties who may or may not have a bank account with that bank or another rural bank. Cheques therefore become a prime target of fraudsters. The rural bankers spoken to mentioned that cheque fraud was increasingly becoming a major problem in their industry. Many cases of this type of fraud were described and were pointed to as evidence of this.

Alterations can easily be made to genuine cheques which have been issued to show different recipients or amounts.

Alternatively when a criminal has access to a genuine blank cheque leaflet from a customer's cheque book and can forge the customer's signature a withdrawal can easily be made.

Criminals can also forge cheques fill them out and forge the signature of account signatories and withdraw various sums from customer accounts

Four types of cheque fraud are discussed in this analysis:

7.6.16 Fraud Scenario 16 – Cheque Fraud Variation 1

Fiifi who has an account in a Tarkwa rural bank with a fraudulent cheque for withdrawal

a. He goes to pay into his account a cash cheque he stole. The cheque was originally issued to Kwasi by Ebo with a Tarkwa rural bank cheque. Fiifi endorses the cheque to show that it was issued to him. A cash cheque is a cheque which is issued and signed but does not bear the name of the recipient hence Fiifi by endorsing with his name it shows the cheque was issued to him.
b. Fiifi forges a Tarkwa rural bank cheque in the name and account number of Ebo. He also forges Ebo's signature and goes to Tarkwa rural bank to make a withdrawal.
c. Fiifi Steals a blank cheque leaflet forges Ebo's signature and fills it to show the cheque was issued to him by Ebo and pays it into his bank account.

With this fraud Fiifi is known to the bank and if the cheque is not found to be fraudulent before being paid then it would be successful. For bank staff to detect the cheque as fraudulent as in the third variation of the fraud, they must detect that the signature is forged. This is the same in the second variation but in that case the bank staff must also detect that the cheque is also forged. Detecting both variations of fraud would depend on the ability of the bank staff to identify the forgery. With the first example unless Ebo finds the cheque is missing and reports it to the bank before Fiifi presents it nothing can prevent it from succeeding. In all three cases Fiifi is known to the bank and if his identity details are correct he could be traced but if the amount it big then he could just go out of town in order not to be arrested.

The major weaknesses here is the ability to detect the document, in this case the cheque, is fraudulent. Then there is the problem of the verifying whether the cheque was truly issued by the account holder.

7.6.17 Fraud Scenario 17 – Cheque Fraud Variation 2

Esi who does not have an account in a commercial or rural bank goes to Prestea rural bank to fraudulently withdraw a Prestea rural bank cheque.

a. Esi steals a Prestea rural bank cheque issued to Yaa from Jojo. The cheque stolen in this case is a crossed cheque so bears Yaa's name. She endorses the cheque to show that Yaa has passed the cheque to her to make the withdrawal. She presents the cheque to the bank with her real identity and makes the withdrawal.
b. Esi steals a Prestea rural bank cheque issued to Yaa from Jojo. The cheque stolen in this case is a crossed cheque so bears Yaa's name. She forges an identity document to claim to be Yaa and presents herself to the bank with her forged identity to cash the cheque.
c. Esi steals a Prestea rural bank cheque issued to Yaa from Jojo. The cheque is a cash cheque and so does not bear Ama's name. She endorses it to show it was issued to her and then makes the withdrawal.
d. Esi forges a Prestea rural bank cheque issued in the name and account number of Jojo to Yaa from Jojo. She forges Jojo's signature on the cheque, fills the cheque in and presents it to make a withdrawal.

This scenario has similar problems with verifying the signature and the authenticity of the cheque as in scenario 16 however this time the perpetrator does not have an account with Prestea rural bank and so it makes it more difficult to trace her if the transaction is later found to be false.

7.6.18 Fraud Scenario 18 - Variation Cheque Fraud 3

Fiifi who has an account in Tarkwa rural bank goes to Prestea rural bank to withdraw a fraudulent Prestea rural bank cheque.

a. Fiifi Steals a cheque issued to Ebo by Jojo with a Prestea rural bank cheque from a rural bank but endorses to show that Ebo has passed the cheque to him (Fiifi). He therefore presents himself to the bank with his real identity to cash the cheque.
b. Fiifi forges a cheque in the name and account of Jojo. He fills it and signs it and presents it to Prestea rural bank to make a withdrawal.

This scenario, just like scenario 18, Fiifi is not known to the Prestea rural bank though he is a customer of Tarkwa rural bank. Tracing him would be very difficult to do

7.6.19 Fraud Scenario 19 – Cheque Fraud Variation 4

Aside a cheque or signature being forged, the amount can also be amended to increase it. Fiifi is an employee and does transactions on behalf of Ebo. She is therefore known to the bank staff as someone who does transactions for Ebo.

a. Fiifi is Ebo's employee who has been issued with a cheque from his employer. He alters the original amount of five thousand to fifty five thousand. This he does by adding the word fifty to the amount in words and the Arabic numeral 5 to the amount in numbers to increase the value. He then withdraws an amount higher than originally intended from Ebo's account.
b. Fiifi steals a cheque from employer Ebo writes it and forges Ebo's signature and presents the cheque to Yaw (a teller) and to cash it.

c. Fiifi steals a cheque from his employer Ebo writes it and forges Ebo's signature and pays it into his account.

In this scenario the cheque is an authentic document and Fiifi who has done many of such transactions uses his real identity to commit the fraud. The main deception is to assume the authority that Ebo gives to him but in this case has not been given the authority.

7.6.20 Fraud Scenario 20 Customer repudiation

Ebo gives a cheque to a third party customer Kwasi to make a withdrawal from his account. Ebo then comes to the bank to deny writing the cheque and demand to be reimbursed.

Employees of the bank spoken to during the field work said in the event of a suspected fraudulent cheque transaction the cheque leaflet and cheque number are checked to verify whether it is a genuine cheque leaflet. Then they also check the signature to verify whether the customer issued the cheque. They can in the case of a forged cheque eventually determine it is forged but it is very difficult. In a specific fraud incident that happened in a commercial bank and recounted during the field research, the account holder due to ill health had signed blank cheques for a family member. This was stolen and the amount filled and presented. The withdrawal was successful because the signature was in fact that of the customer.

Though customers are responsible for their chequebooks it is also the banks responsibility to prevent fraudulent withdrawal from customer account. It is therefore important that banks be able to ensure that customers do not deny transactions they themselves have requested for.

7.7 Pattern in Fraud Scenarios

After a critical analysis of the rural banking processes and scenarios it is evident that the risks faced by rural banks are a combination of transaction, identification based failures and document fiddling.

Fraud Goal	Financial benefit of the actor
Actors	Employee – Internal operative Customer – Account holding and non account holding
Fraud Target	Identity, transactions, documents
Fraud Technique	Assuming a false identity and or false authority to enable transaction execution.

Table 7.1 Rural Banking Fraud Model

The rural banking fraud model showed in table 7.1 indicates the essential elements of fraud within rural banks. The scenarios showed weaknesses in controls, poor separation of duties and the inability to tie incoming cheques or source documents to transactions. It also showed that these weaknesses lead to transaction without source documents, impersonation, fraudulent gaining authority, forged cheques and altered cheques and the use of false identity. Table 7.2 shows a summary of the fraud scenarios discussed in this chapter.

Fraud Scenario	Perpetrator	Methods for Deception	Targeted Step
Unauthorised withdrawal	Employee	Perform transaction without valid request	Source document
Unauthorised Loan	Employee	Perform withdrawal feigning customer phone request	Source document
Same day reversal	Teller	Perform transaction reversal with false premise	Transaction reversal
Job rotation	Employee	Opening customer account with a fictitious identity	Identity verification during a/c opening
False cheque book request	Front office clerk	Fictitious request of cheque book	Source document
Signatory alteration	Front office clerk	Fictitious change of signatory to customer account	Source document
Money transfer	Front office clerk	Impersonation for money collection	Transfer of transaction details
Account opening	Front office clerk	Refusal to pay in initial deposit	Initial paying in of deposit
Systems admin login	Systems Administrator	Accessing login details	Access to login details
Dividend payment	Back office clerk	Paying dividend into different account	Crediting beneficiary account
Suspense account	Back office clerk	Withdrawal or transferring money to wrongful recipient from suspense a/c	Crediting beneficiary account
Teller till	Teller	Withdrawal from teller till	End of day processes
Cheque kiting	Account holding customer	Gaining trust of manager	Withdrawal from account
Account opening with false ID	Account holding customer	Identity fraud	Identity verification during a/c opening
Employee ID	Job Applicant	Identity fraud	Identity verification during recruitment
Cheque Fraud 1	Non account holding customer	Forged cheque	Cheque of authenticity of cheque
Cheque Fraud 2	Non account holding customer	Impersonation of cheque beneficiary	Verification of authority of cheque holder
		Forged cheque	Cheque of authenticity of cheque
Cheque Fraud 3	Non account holding customer	Impersonation of cheque beneficiary	Verification of authority of cheque holder
		Forged cheque	Cheque of authenticity of cheque
Cheque Fraud 4	Non account holding customer	Amendment cheque details	Cheque of authenticity of cheque
		Forged cheque	Cheque of authenticity of cheque
Customer Repudiation	Account holding customer	Repudiation of transaction	Verification of authorisation to perform transaction

Table 7.2 Summary of Fraud Scenarios

All the frauds described in the scenarios occur when fraudsters take advantage of weaknesses to mismatch items in the two different spheres of the rural bank operations. As can be seen in the scenarios rural banks work in two spheres first the physical actors or tokens and their representation in the form of records tracking them as shown in Figure 7.2.

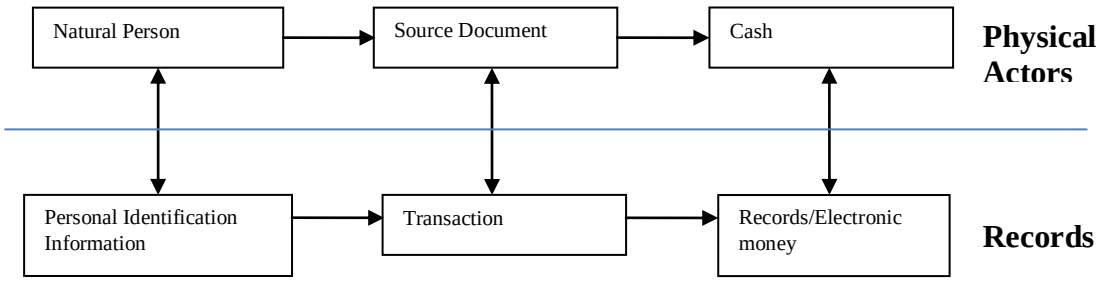


Figure 7.2 Interactions Between Actors in Banking

There is for example the human person and the personal identifiable information kept as the identity of the person in the bank. On the other hand there are source documents and the transactions processed. Then there is the cash and the amount stored on record. Deception leading to fraud is able to occur when these two aspects do not match. For example when a fraudster is able to claim an identity either at the account opening stage or job application or impersonate a customer whose identity has been created and stored in the banks records.

Since people are offered certain benefits because of who they are, being able to impersonate a person accrue these benefits to the impersonator. On the other hand banks offer benefits to people on the basis of documents in their possession and if these documents get into the hands of fraudsters they acquire the ability to access these benefits. In the same way fraudsters could get access to physical cash without detection if it does not show in the record of the cash kept in the bank. Such cash could be used and returned without it being discovered.

All these are able to occur because there is a disconnect between the physical part of the system and the records electronic or otherwise. Table 7.3 shows the summary of the physical elements and the records that represent them.

Physical element		Record
Natural Person	Account Holder	Identity information
	Non Account Holder	Identity information/document (e.g. ID card)
	Employee	Identity information
	Photographs	Identity
	ID Cards	Identity
Source Document	Cheque	Withdrawal Transaction
	Internally Generated Voucher	Credit/Debit Transaction
Cash	Cash in Vaults	Cash Account balance
	Cash in Till	Till Account balance

Table 7.3 Physical Elements and Records Representing Them

Fraud is able to occur in the rural banking system because there seem to be a disconnect between the various components of the system that runs the banking system. The first as mentioned is the disconnect between the banking processes and the documents used to initiate the processes then fraudsters can perform the process without a document. There is an opportunity to commit fraud if a transaction can be processed without a valid document to back it. There should be a reliable mechanism that can verify and tie source documents to relevant steps of the transaction such that the transaction cannot be executed unless a there is a valid supporting document.

The second is the inability to reliably connect an identity within the banks records or the personal identification information to a natural person. This inability creates the opportunity for impersonation.

The final one is the inability to match the physical assets in this case cash with the records on banks records. An insider to the bank can therefore take cash from the bank and return it at a later date without detection because the bank records would show that the right amount of cash that is supposed to be there but in reality it is less.

The other risks present are that preceding subjects or objects are not verified properly before subsequent subjects or objects. For example it must be objectively verified that

an account holder issued a cheque before a withdrawal is made to the account. It is therefore critical that preceding subjects be objectively verified before the next subject can be verified in a chain of transaction. This mechanism should be able to verify whether a subject has been authorised or not to initiate or execute a transaction.

Any design to deal with fraud should be able to deal with these fundamental issues. The first is to match the physical elements in the banking processes to the records. The second is to be able to ensure that preceding events are objectively true before a subsequent event can proceed.

Chapter 8

8 Rural Banking Integrity Model

This chapter discusses the Rural Banking Integrity Model (RBIM) which is the fraud protection model that is proposed to deal with the weaknesses within the rural banking industry. It introduces innovative mechanisms incorporating some information security techniques which are aligned to the culture of the community. It makes use of traditional community structure and the adinkra symbols to achieve identity certification and verification.

8.1 Fraud Control Requirements

In order to deal with the weaknesses identified in the last two chapters there are certain requirements that must be met. These are as follows;

- Ensuring that identities are reliably verified. Verification of identities would be done by reliably linking the identity of a customer of a bank to the natural person.
- Ensure that only the rightful customer or bank official can initiate a transaction by linking the verified identity to the documents purported to come from them. This is also to ensure that documents used to initiate transactions are not forged and are issued by genuine customers or officials of a bank. To achieve this,

customers must to be tightly tied to documents and documents tied to transactions. This means that if one element in the chain is false a transaction cannot proceed.

- Ensuring authorised employees are the ones performing transactions
- Ensuring that there are not conflicting tasks performed by employees

8.2 Rural Banking Integrity Model

The rural banking integrity model has four main parts namely Community Based Identity Certification, Identity Verification, Authority Verification and Transaction Security as shown in Figure 8.1

<table>
<tr><td rowspan="2">Identity Certification</td><td colspan="5">Community Based Identity Certification</td></tr>
<tr><td rowspan="2">Identity Verification</td><td colspan="2">Digital Certificate</td><td colspan="3">Transaction Authentication Number system</td></tr>
<tr><td>Authority Verification</td><td colspan="5">Transaction Verification Number System</td></tr>
<tr><td>Transaction Security</td><td>Static Separation of duties</td><td>Dynamic Separation of duties</td><td>Object based Separation of Duties</td><td>Atomicity</td><td>Account Transfer Keys</td></tr>
</table>

Figure 8.1 Rural Bank Integrity Model (RBIM)

The Community Based Identity Certification requires a customer to have his identity certified and a certificate issued before an account is opened for them. This is done by using a certified community leader to give an identity reference. Having an identity certificate is therefore a necessary condition before an account is opened or a transaction is processed.

Identity verification includes mechanisms designed to verify identities of customer when they request a transaction. When a certified customer returns to the bank for a transaction their identities are verified when they produce a valid Personal Identification Code (PIC). This is a set of four Adinkra traditional symbols provided in a serial order. For a third party customer, transactions can only proceed if a valid one time use Transaction Authentication Code (TAC) is used to show authorisation from the legitimate account holder. This is also asset of four Adinkra symbols.

Authority verification involves verifying the authenticity of source documents. Every genuine document must have a Transaction Verification Code (TVC). A TVC is a machine readable random number printed on bank issued documents.

While a PIC/TAC and a TVC are necessary conditions individually. A combination of a valid PIC/TAC and a valid TVC is the sufficient condition for a transaction to be initiated.

Transaction security ensures the transaction processes are not manipulated. It involves separation of duties, account transfer keys and atomic transactions. When a transaction is initiated, there must be a satisfactory static, dynamic and object based separation of duties before it can proceed. In a case when it cannot be met, the necessary authorisation must be sought for it to be completed. Account transfer keys which are public keys are used to ensure payments made can only be paid into the intended account. Finally atomicity is used to ensure that a minimum number of tasks must be completed for a change to be effected in transactions.

In the RBIM the customer, employee, document and transactions are validated before a transaction can be executed.

8.3 Design Principles Adopted

In designing a model to maintain the integrity of rural banking operations, several concepts have been adopted. The integrity model is essentially a role based access control system. However it incorporates concepts from other information security models including the new access control model for data mining environments which is a variation of the Chinese wall security policy and the Aggressive Chinese Wall Security Policy.

This RBIM has been designed to meet the requirement of the Clark – Wilson model. However it also prescribes innovative ways of achieving optimum protection within the Clark – Wilson model whilst effectively meeting the security requirements of rural banks. This is done in cases where the Clark – Wilson model seems inadequate or lacking detail in dealing with certain aspects of risks faced by the banks. The Clark – Wilson Model for example does not do much with regard to human identification which has been shown as a key target of fraudsters. The rural banking integrity model prescribes new ways to meet this requirement which is crucial but intricately linked to the success of transaction protection mechanisms.

In addition to the role based controls, it also implements various other levels of control. At the base, general privileges are assigned to all users depending on their role and the assignment of these privileges must meet the static and dynamic separation of duties requirements and also meet the least privilege security rule.

The integrity model however uses other mechanisms to meet additional separation of duties requirements to restrict the use of the privileges. It therefore operates at a higher level of granularity during operation in controlling the use of privileges using various

parameters. This higher level of control supersedes a user's assigned static and dynamic privileges that go with roles. Controls are determined for every instance of request made by a user to use a transformation procedure. This is done because role based access control do not by themselves have the ability to deal with complex issues which organisations have, there is the need to go beyond access control mechanisms and make rules which addresses security issues (Farraiolo and Kuhn, 1992) hence the integrity model use of additional customised controls which are to be discussed shortly.

To ensure the best possible design, the eight design principles are recommended for designing protection mechanisms (Saltzer and Schroeder, 1974) was adopted. These principles have been taken into consideration in the design of the protection mechanism. They are;

1. Economy of mechanism: Keep the design as simple and as small as possible.
2. Fail-safe defaults: Base access decisions on permission rather than exclusion.
3. Complete mediation: Every access to every object must be checked for authority.
4. Open design: The design should not be secret.
5. Separation of privilege: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
6. Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
7. Least common mechanism: Minimize the amount of mechanism common to more than one user and depended on by all users.

8. Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

8.4 Key strengths of the Integrity Model

The key strengths of the model are its strong identification mechanisms which matches the identity of a person with the natural person.

The integrity model is also strong on preventative action on fraud by verifying the identity and authority of an account holder or the employee who is performing the transaction before a transaction can proceed. Not only does it have mechanisms that verify the credential of the returning customer but also reliably certify that the identity being used is the legal identity of the natural person.

The model uses well formed transactions and various mechanisms to prevent complex fraud which in some cases are committed using more than one process. It also incorporates various mechanisms that ties documents to transactions and verifies the authority of customers requesting transactions on another person's account.

8.5 Role of ARB Apex Bank

The main role of the ARB Apex bank serves as a certification and facilitation body for the RBIM. With the reach of the ARB Apex bank its participation could be crucial in supporting rural banks secure transactions by creating a structure to aid sharing of risk information between rural banks. One of the main roles the ARB Apex bank is expected to play in the RBIM is that of identity verification and management. This is discussed in the next section.

Rural banks perform many transactions that go across their own organisation's boundaries and through the ARB Apex bank. Though these transactions may not begin and end in the ARB Apex bank and so they do not have end to end control they can play the role of collecting, comparing and identifying anomalies in transactions. Information regarding risky customers and risky employees could also be shared to help reduce operational risk and fraud. This is because it provides a central point for rural banking through its services and its oversight function. A centralised security program provide increased efficiency and economy of security throughout the organization and the ability to provide centralized enforcement and oversight (Swanson and Guttman, 1996).

The ARB Apex bank as discussed in chapter 5 holds accounts for rural banks and they also perform clearing between rural banks and take other commercial bank cheques for clearing at bank of Ghana on behalf of rural banks. They also support banking operations of rural banks and though apex bank is not involved in non-prudential regulation, their role in setting rural banks for secure operations can be critical to its success.

8.6 Community Based Certification

One of the key elements of the RBIM is identity certification. Identification of users in the rural banking systems as has been mentioned earlier is woefully inadequate. In performing customer due diligence the customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered to determine how risky the customer is (Working Group on Crossborder Banking, 2001). It is also recommended that banks should develop graduated customer acceptance policies and procedures that require more

extensive due diligence for higher risk customers. Though these recommendations are originally aimed at prevention of money laundering it is very relevant in the fight against fraud. Banks are therefore encouraged to satisfactorily verify the identity of their customer.

In the case of services like the Home cash/*efie ne fie* (see chapter 6) where customers open accounts from another bank, mechanisms are needed to ensure that due diligence are done properly. Rural banks must not rely only on the due diligence done by the bank where the prospective customer lives but must also be able to independently verify the identity of the prospective customer. Initial identification mechanism done with a community based identification mechanism to be discussed shortly should be able to deal with this. With the reach of the ARB Apex bank, its role in bringing together information from various locations could be key to ensuring proper due diligence is done.

As discussed in chapter 3, rural communities form the basis of the identity of almost all Ghanaians. Rural banks can therefore tap into this social system for the purpose of identifying and assessing the risk rating of prospective customers. Figure 8.2 shows the actors of the community based certification system.

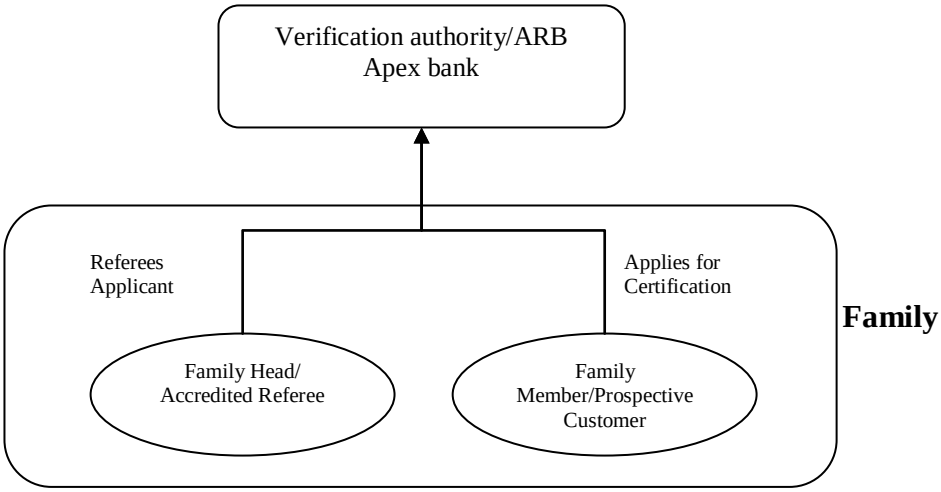


Figure 8.2 Actors in Community Based Identification

Every family has a family head and families are keen to have the respect of the community. The design of the integrity model takes advantage of this unique culture to verify the identity and character of a prospective customer by asking the family in the person of the family head to give a reference.

ARB Apex bank would have the role of accrediting the customer through the community scheme and assigning them a risk value. ARB Apex bank would under the community based certification have list of vetted and approved list of community leaders and family heads to represent their families. These vetted leaders would be called upon to identify and verify the particulars of members of their Families who have applied to open accounts with rural banks.

Families in effect stake their reputation on the member being refereed. In so doing, a family refereeing its members will be held liable by being labelled as risky if the refereed member ends up as a fraudster. They would therefore have the incentive not to

endorse a criminal to a bank as it would bring the whole family into disrepute reducing the trustworthiness within the community and with the bank.

It is expected that people who have moved from their original home towns could still take advantage of the centralised ARB Apex certification scheme to have their family heads give them a reference.

In a case of where people cannot use their families for certification community leaders of acceptable identifiable groups could be used as a mechanism for referencing. In marketing towns for example there are marketing associations with identifiable leaders. These organisations could give a group reference to their members but that would mean that they would be staking their reputation on the line when they give a reference to a person.

The logic here is that the level of reputational risk to a family or a community grouping must be commensurate with the risk rating the bank would assign to the person being assessed.

When a prospective customer is certified an electronic identity certificate would be created and stored on a secure server on at the ARB Apex bank. This is to ensure higher security and to enable other rural banks to access these certificates for the purpose of identification where customers of one bank go to another rural bank to perform a transaction.

Each customer must therefore have an electronic certificate which would bear the name, photo, address, account details and the level of risk that the customer poses to a bank. This certificate is necessary before an account is opened and would be available to all rural banks.

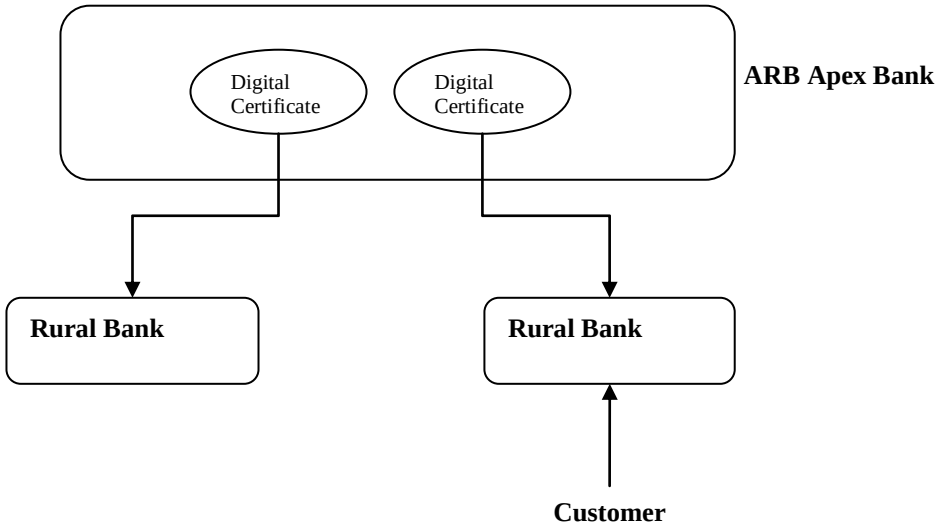


Figure 8.3 Verification of a Certified Customer

When a certified customer goes to a bank his identity will be verified with an electronic certificate which is created during the initial community based certification system discussed in the previous section. As mentioned earlier rural banks are limited to specific localities and therefore needs ARB Apex bank as an intermediary when they have perform transactions which involve different localities.

Figure 8.3 illustrates the verification of a certified customer's identity. Currently if a customer of one bank goes to another bank to perform a transaction the customer has to provide identification to the bank as a non customer would. In the case of the RBIM, if the customer has been accredited by the ARB Apex bank then the customer can use this accreditation to certify their identity.

8.7 Customer Authority Verification

The RBIM uses the Personal Identification Code (PIC), Transaction Authentication Code (TAC) and the Transaction Verification Code (TVC) to verify the identity of

customer and source documents. Currently when an account holding customer goes to the bank, identification is by the matching the person to a photograph. For the bank's customer the photograph which the bank matches against the person is what was provided by the customer during account opening and is already on their system. This mechanism is maintained but in an enhanced form where the digitised photograph of the certified customer is kept on the secure ARB Apex bank server and retrieved for use by rural banks. To ensure the transaction has been initiated by the legitimate customer and Personal Identification Code (PIC) is required to be entered by the customer.

The RBIM introduces the Transaction Authentication Code (TAC) to identify non account holding customers. Currently they do not have photograph with the banks, so documents like a passport or a voter's identification card with a photograph is required. Passport and other government issued documents have been shown earlier to be unreliable in chapter 5. They in most cases represent a single point of failure since they are trusted to be reliable documents but are not.

Transaction Verification Code (TVC) is the means introduced to verify source documents. Currently the only means verifying whether a cheque is genuine is the customer's signature and cheque number. Now as mentioned in the fraud scenarios in chapter 6, if a person presents a fraudulent cheque to cash at a rural bank, a Forged ID document or a "genuine" ID obtained with a false identity there would be no way to trace this person except.

As discussed in chapter 3, the Clark-Wilson model indicates that separation of duties requirement should insist the initiator of a well formed transaction be different from the executor. In the case of rural banks there isn't a reliable way to verify that the

transaction was truly initiated by the genuine customer due to the highly unreliable means for verifying a customer's identity. In addition an employee can masquerade as a customer and an employee to initiate and execute a fraudulent transaction as shown in scenarios 1 and 2 in chapter 6.

Mechanisms are therefore needed to deal with this serious flaw where the bank cannot reliably identify the transaction originating customer. The integrity model looks at various ways that people can be identified more reliably using one time use Transaction Authentication Code (TAC). It also uses the Transaction verification Code (TVC) to reliably verify that documents authorising the initiation of transaction are genuine.

8.7.1 Personal Identification Code /Transaction Authentication Code

The concept of a PIC/TAC is basically verifying authority to perform a transaction on an account by what you know based on the adinkra symbols. Being a set of pictorial traditional symbols it is expected to be easier for the rural community to use than Arabic numerals because majority of the rural population are illiterate.

Certified customers will have a PIC which is unchangeable. This is a four adinkra symbol code that certified customers will use to identify themselves every time they go into the bank. Third party customers on the other hand will use a onetime use TAC for verification of third party customers and to confirm they have the authority to perform the transaction. Certified customer are customers who have been certified by the ARB Apex bank using the community based identity verification system. Third party customers on the other hand are customers requesting transactions on accounts which are not theirs. A TAC is also set of four Adinkra symbols. Figure 8.4 shows the operation of the customer verification processes.

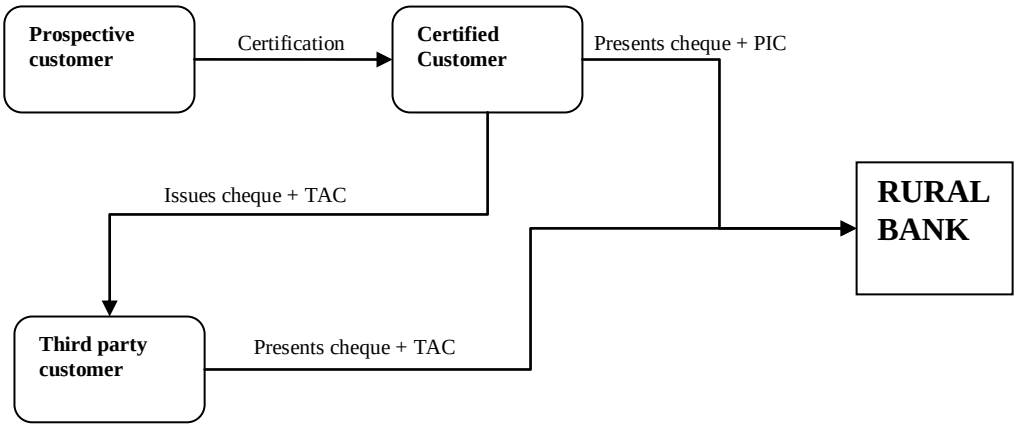


Figure 8.4 Customer Identification Verification System

There are a total of eighty of these symbols representing various aphorisms. The RBIM however will use twenty symbols that are most used by artisans like traditional jewellers and printers. The principle of the TAC is that when a third party customer requires performing a transaction on another person's account, they need to show prove authorisation from the account holder. This is done by presenting a valid TAC for verification.

An account holder would be issued with a unique set of TACs for the purpose of identifying third party customers. The objective of TACs is to help employees identify who has legitimate authority to request a transaction on an account. This would prevent criminals be it employee or an outsider from cashing fraudulent cheques either in the form of a forged leaflet or by stealing a genuine leaflet and forging a signature. To cash a fraudulent cheque a criminal would have to breach the cheque security, be able to forge a signature and breach the TAC security.

When a cheque is issued to a third party the customer gives the cheque recipient a TAC which is an authentication number to present along with the cheque to the bank. This person presenting the cheque enters the TAC by pressing a combination of Adinkra symbols on a key pad in the particular order given. The TAC is then hashed and matched with the hashed value linked to the specific account on the banks secure server.

PICs are used in the same way as a TAC but since it is a code for the certified customer it does not change with every transaction. When a certified customer goes to a bank they enter their PIC and the hashed value is matched against that stored on the banks secure server for the said identity and account.

One time use TACs are random numbers translated into sets of four Adinkra symbols and issued to customers. Each Adinkra symbol will be given a numeric value hence when it is entered onto a keypad it is translated into a number for hashing. TACs are to be issued separately by the bank to customers and a one way encrypted version is kept on a secure server in the bank and tied to a customer's account. TACs would not be linked to individual cheques because it is not meant to verify a cheque. TACs would be issued separately in batches to the account holder to be issued randomly to third party customers by the account holder as a means of verifying their authority to perform transactions on their account.

TACs are therefore going to prevent fraudsters using deception to assume the authority to perform a fraudulent transaction.

Also using the twenty most used symbols to create the TAC identification system would give a total of 20^4 possible combinations giving a total of 160,000 TACS! The

probability of guessing a TAC is 0.00000625 and far lower and more secure than the current 4 digit PIN system in use.

8.8 Customer Authorisation and Transaction Verification Code (TVC)

The transaction verification code (TVC) is used as a means to verify the authenticity of cheques and to avoid forgery which banks officials claimed has recently been on the increase. Fraudsters have been able to reproduce cheques which bank employees have not been able to detect. In the RBIM model every cheque would bear a TVC which is a machine readable number randomly generated and printed on the cheque. When cheques are presented they would be scanned to read TVCs which would be hashed and matched to numbers on a secure server in the banks for authorisation before transactions can be processed. Generating TVCs would be done by an automated system writing the hashed version on to the customer's account whiles electronically transmitting the plaintext version to secure printers to be printed on cheques.

8.8.1 TVCs, Transaction Authentication and Non repudiation

The other main objective of a TVC is to prevent account transactions without a valid paper trail (cheque). A transaction without a valid TVC cannot proceed. It therefore increases the difficulty for an employee of a bank to fraudulently withdraw money from customer account without the customer's cheque. Even if an employee has the relevant permissions assigned to make an account withdrawal, it cannot be done without a valid TVC.

One other objective is to reduce the likelihood of non repudiation. Transactions can only be performed on an account with a document with a valid TVC. Hence for a transaction to have been performed then it is almost certain that the cheque is a genuine

leaflet from the customer's cheque book. Combined with third party identification procedures (See TAC) in the model it can be verified whether a cheque was cashed by the customer or a third party.

8.9 Transaction Security

In the RBIM users are only allowed to modify data with a well formed transaction. Well formed transactions prevent users from entering or modifying information within an information system in an arbitrary way. The two main ways where integrity can be achieved in commercial system involves the use of a well formed transaction and separation of duties (Clark and Wilson, 1987). Well formed transactions preserve the integrity of information and keep enough data on transactions to be able to reconstruct the transaction.

Various mechanisms in addition to the identity management mechanisms described above are considered to help achieve this property. They include separation of duties, atomicity and public key encryption.

Just like in the Clark – Wilson Model, the RBIM uses the structure of the transaction to ensure internal consistency of the information stored on computer systems.

Separation of duties is a mechanism that prevents having several tasks in a transaction fall into the hands of an individual. It is a mechanism aimed at ensuring the correspondence of data objects within an information system and the real world objects they represent (Clark and Wilson, 1987 , Nash and Poland, 1990).

8.9.1 Separation of duties and fraud prevention

As mentioned earlier the integrity model implements separation of duties in three forms namely static and dynamic separation of duties to ensure that possible fraud within the same transaction does not occur. In these two forms of separation of duties conflicting tasks in a transaction must not be assigned to the same role. Secondly, where an individual is assigned more than one conflicting permissions then the conflicting permissions must not be executed within the same transaction.

The third is an object based separation of duties constraint that has to do with the use of conflicting tasks on the same object. This introduces some Chinese wall policies into separation of duties. An individual cannot execute two conflicting permissions in different transactions on the same object.

8.9.1.1 Static separation of duties

As is currently in rural banks, there are certain tasks that would hardly be assumed by certain types of staff. An example would be the authorization role of the manager would never be assumed by a clerk. There is no justification in including these permissions in a clerk's set of permission in a role based access environment that the integrity model operates. Since tasks like these are permanently in conflict and would never overlap they are separated by static separation of duties mechanisms.

8.9.1.2 Dynamic separation of duties

On the other hand there are roles that can easily be assumed by clerks in a situation say when a colleague is taken ill and cannot turn up for work. It is prudent to put these mutually exclusive permissions in the same role but to regulate their use with dynamic separation of duties mechanisms which would prevent a user from exercising two or more mutually exclusive permissions in one transaction.

8.9.1.3 Object based separation of duties

The integrity model uses object based separation of duties to prevent possible fraud occurring using more than one unrelated transaction. This form of fraud prevention technique does not automatically prohibit certain combination of transactions, rather tasks are deemed conflicting based on the context. In such a case where two or more tasks are thought to be conflicting additional authorisation and controls would kick in before the transaction can proceed.

Implementation of object based separation of duties in the integrity model introduces elements of the Chinese wall security policy which excludes a user from certain privileges based on the user's prior activity. Object based separation of duties is used to regulate situations when users exercise permissions which have been legitimately assigned but creates a conflicting situation when used on the same object. Such permissions could be in mutually exclusive roles in separate transactions at different times hence would not be picked up in static or dynamic separation of duties.

There are known cases where employees have used the assigned permissions legitimately when in one role and also exercised other permissions legitimately in other roles but together these permissions exercised on the same object poses a security risk. An example of high profile fraud perpetrated using normally non-mutually exclusive transactions is the Mckenzie Bank of Scotland fraud case (Lister, 2006 , BBC, 2006). Mckenzie opened fictitious accounts and then used then to apply for loans totalling £21 million.

With rural banks using job rotation as a means of ensuring security, there is a high risk of employees using the various positions assigned to them and the permission that go

with them to perform various transactions to commit fraud or as a cover up of fraudulent transactions.

In object based separation of duties employees (subjects) are unauthorized to perform transactions on accounts (objects) that is in a state which might be in conflict with the current transaction. The state of the object is the combination of three elements namely the data object in question, the type of transaction and subject performing the transaction. This is referred to as the RBIM access control triple.

Conflict here is between the history of access control triple with regards to that particular object (customer account) and the access control triples of the current transaction with regards to the same object. The principle of putting together the history of transactions to determine level risk makes use of the principle of aggregation where adversaries put bits of information together to get the bigger picture. Here the focus is on putting transactions together to commit fraud rather than putting data objects together.

Given a state of an access control triple for an object which puts it at higher conflict with a current transaction the implication will be that it is easier for the employee to commit fraud. The level of conflict indicates the level of risk the current transaction poses. If the risk of a current transaction is higher, the level of security requirements for the transaction to proceed would be increased or set to a higher level and would require a higher level of authorisation or scrutiny.

In other words a series of transaction by a subject on an object should determine whether the subject can have further access of a particular type in the future. The issue

would not be who you are but what you have done and whether you have the opportunity to commit fraud.

For a subject S_1 who has performed transactions $T_{(1.....n)}$ on an object O_1, if S_1 wants to perform a transaction T_c, the conflict C will be between the

$$C = f[S_1O_1T_{(1.....n)}] - f[S_1O_1T_c]$$

$$C = f[S_1O_1(T_{(1.....n)} - T_c)]$$

The level of conflict with respect to a specific object and subject will depend on the historical transactions of the subject on the object and the current transaction.

The tranquillity principle is used in dealing with object based separation of duties. It is however not in terms of upgrading or downgrading the security level of the object that has been accessed by a subject. Rather it is used to upgrade or downgrade the level of conflict between a history of a user and a current transaction. When an employee performs a transaction that is in conflict with another transaction, the security requirement to perform the second transaction is increased. Object based separation of duty is to help deal with any opportunity that could arise to commit fraud.

8.9.1.4 Distance and Conflicting Transactions

Distance as used in the new access control model for data mining environments to measure the severity of conflict (see chapter 3). This principle is used to deal with over classification in the RBIM. The problem with object based separation of duties is that employees could easily be eliminated from performing any transactions with time because they would have performed every transaction on an account. In rural banking there are small staff numbers and the implementation of the object separation of duties

constraint could be a serious problem where the transaction history of bank staff can progressively put each member of staff in a position where every transaction is in conflict with the current transaction.

In the object based separation of duties, conflict is determined by the historical transaction by the subject on the object and the current transaction the subject requires performing. So given the historical transaction $T_{1...n}$ and current transaction T_c, the risk rating which depends on the level of conflict which is a function of the two will be;

$$R = f(T_{1...n}, T_c)$$

Where

R = *Fraud Risk*

$T_{1...n}$ = *Transaction history*

And T_c = *Current transaction c*

What is proposed is that aside the subject's transactions there would have been other intervening transactions by other subjects which may reduce the risk. An example will be if an employee opened an account and the customer has been handled by other staff then the risk of it being a fictitious account will be reduced. This is because it is expected that other employees would have verified the existence of the customer. On the other hand if there has not been any intervening transaction which could have possibly answered some questions then it must be flagged as a high risk transaction requiring additional authorisation.

The fraud risk therefore becomes;

$$R = f(T_{1...n,}|O_{H,}\ T_c)$$

Where

R = *Fraud Risk*

$T_{1...n}$ = *Transaction history*

T_c = *Current transaction c*

O_H = *Objects history*

And $T_{1....n,}|O_H$ = *Transaction history of given an object history* (O_H)

As mentioned earlier the level of conflict determines the level of risk and this would be the basis for determining the level of authorisation or scrutiny required to get the transaction in question processed.

Different levels of risk would have a different authorisation requirement. When the current fraud risk is determined the corresponding level of authorisation would be required to ensure the transaction proceeds. Object based conflict rules would be determined to reflect the risk management policies which are based on a risk assessment, risk rating of the staff and other prevailing factors like the number of staff etc.

8.9.2 Atomicity in Transactions

The concept of splitting a transaction process into smaller tasks with each task given to a separate person has been shown to be a reliable security mechanism. However there are risks that arise when the breaking up of transactions create risk transactions that

give criminals the opportunity to commit fraud. These transactions are able to bypass controls and give opportunity for fraud.

The integrity model therefore has an atomicity requirement. This requires a minimum set of subtasks to be completed before a task is deemed valid. An atomic task should include enough sub tasks to ensure that all any information entries or changes on the computer system matches real world objects they represent and the intensions of all stakeholders of the objects.

8.9.3 Account Transfer Keys

Interbank and inter account transfers were also identified as a source of fraud and it is important to ensure that inter account transfers do not end up in the wrong as a result of errors or a deliberate attempt to commit fraud.

A public key encryption protocol is a reliable way to achieve this. When a customer requires to make an inter account transfer in the same or different bank, the recipient would in addition to giving the customer an account name, the bank branch and an account number, an account transfer key (ATK) which is the recipients public key. The recipient bank branch code, recipient account holders name and account number, senders name and amount would be encrypted and sent over the network.

When the message is received it would be decrypted with the accounts private key and can only default into the right account. If the details do not match to an account then the transfer would be rejected and returned immediately. Also to achieve optimum results it would require the payee to personally enter the ATK. This would eliminate the risk of the employee entering the wrong key.

8.10 Validation of RBIM

As discussed earlier, security requirements could be validation to ascertain that the right system is being built and that the system implements the requirements. A validation process could be done formally or informally. Validation is necessarily an informal process since only human judgment can determine if the system that was specified and built is the right one for the job (Kuhn et al., 2003).

The RBIM was validated informally using rural and commercial bank staff. Brain storming was used as an informal means to discuss the model and to refine it. The final model was then informally validated by running the fraud scenarios discussed in chapter 6. This was done to see how the RBIM will deal with those of fraud scenarios. Generally the RBIM had mechanisms to deal with all the fraud scenarios except for one. This was fraud scenario 19A. Also fraud scenario 19A was not prevented because the RBIM could not detect the amendment of the amount on a cheque which has been issued to a third party.

The validation process involved two discussions each with four rural bankers and a one commercial banker. A total of 10 discussions were made with five members of staff aimed at refining the model and the other five aimed at validating the design. Various suggestions were made during the discussions and amendments were subsequently made to the original designs. The designs changes include the inclusion of a PIC to eliminate the weakness of using a photograph and a signature for identification and verification of a certified customer.

The various fraud scenarios and the mechanisms that deal with then have been shown in a table in Appendix E. This table shows the weakness in the system that enables the fraud to take place and the prescribed mechanism to deals with it.

8.11 In Summary

The Rural Banking Integrity Model was presented in the chapter as it presents a simple fraud control model that is aligned to the culture of the rural Ghanaian community. It presents a robust identity certification system that uses traditional community structures. It also presents the use of authentication codes that uses traditional pictorial symbols that can tie the various elements within the banking system. Other mechanisms together with the ones mentioned earlier are used to reduce deception that lead to fraud are also presented. Informal validation showed the RBIM to be an effective design that can deal with fraud.

Chapter 9

9 Conclusions

The research concluded that conventional risk management and fraud and banking controls would not work in the rural banking industry in Ghana and that the Rural Banking Integrity Model as a fraud control model that is designed to meet the needs of the rural banking industry.

The research work has covered various aspects of fraud and fraud control in the Ghanaian rural banking industry. Fraud was dealt with as an operational risk problem and it was therefore looked at from the point of view of business processes that deliver rural banking services. As was shown during discussions, a holistic view was however taken analysing the rural banking system and its environment. All the questions that the research sought to answer were adequately answered and it presented a better understanding of the manifestation of the nature of fraud.

9.1 Nature of Rural Banking Industry

During the course of the research work the rural banking industry was critically analysed. It was shown that the industry is unique and that has it has its strengths and weaknesses. A discussion of the regulatory framework revealed that it primarily

determines the nature of rural banking. It does that by restricting its operations in terms of geographical location and the type of business operations rural banks can pursue. Other characteristics like the structure of the industry and individual banks was shown to have an impact on fraud and the effectiveness of fraud control mechanisms like separation of duty.

It was clear that conventional banking controls cannot be effective against fraud in rural banks due to various reasons. Conventional practices have their weaknesses and also the nature of the rural banking system make it difficult to use these practices. Some of the weaknesses identified in conventional banking control were the unreliability of signatures, cheques and the ability to circumvent controls. Other weaknesses that were as a result of the nature of the rural banks and these include the absence of street names and fixed addresses and documents like bills as a means of identity verification, unreliability of photo ID documents in Ghana. It was also seen that the lack of education and familiarity with technology could be a disadvantage in implementing certain mechanisms.

Due to the nature of the rural banking industry there is some systemic vulnerability that makes it difficult to implement conventional fraud control mechanisms. Some of these weaknesses are that banking processes had to cross organisational boundaries making it difficult to assign control responsibility. The other weaknesses involve small staff sizes of rural banks which reduce the ability to use separation of duties thought to be critical to fraud control. The environment of rural banks was also critically discussed as a source of threat and opportunity to dealing with rural banking fraud.

9.2 Scenarios

The research was able to identify various ways in which fraud could be manifested within the rural banking industry. In doing so 20 fraud scenarios were presented with

the help of the experienced bankers in the industry. In analysing how these scenarios could be perpetrated it was realised that the lack a reliable tie between the physical elements of banking operations and the records was the main problem that enabled fraudsters to create a deception for the fraud.

9.3 Annual Loss Expectancy (ALE) Model

The ALE which is a main means for assessing risk was not used in the study of rural banking fraud risk. The ALE model involves assessing risk in terms of its likelihood and impact. This model was however thought to be inappropriate for this purpose mainly because there is a wide range of fraud risk events that could occur and historical events could not be used a means of predicting future events. Therefore to use the ALE model would involve mainly subjective values. A vulnerability analysis was rather used to determine all reasonable weaknesses. A holistic fraud mitigation system was then developed. This method was desirable because weaknesses can be exploited in different ways to commit fraud and dealing with the weaknesses deals with the various known and unknown forms it can be exploited.

9.4 Fraud Control and Security Models

It is proposed that internal controls which is the best means for dealing with fraud is best implemented when users cannot have the discretion to abide by it or not. Further to this, information security is put forward as the best means to enforce internal controls in a computer dependent industry like banking. It therefore suggests that computer security techniques must be seen as a tool in the managing operational risks.

Several security models were analysed as a means analysed to adopt useful mechanisms to develop a fraud control system. The role based access control

framework and the Clark-Wilson security model informed much of the design of the rural banking integrity model however many other security models provided useful techniques to deal with risks identified. Mandatory and discretionary access controls were discussed. Mandatory access controls were thought to be more appropriate in enforcing a fraud control system and to enforce organisational policy than a discretionary access control models.

Whilst multilevel security was originally developed for military systems it has various principles like over classification and tranquillity that were useful in the development of the RBIM. Other multilateral security principles as implemented in the Chinese Wall Security Model and its derivatives also provided useful techniques for dealing with separation of duties issues.

As was shown in chapter three, role based access controls reflect the nature of organisations and so gives a good means for structuring security controls. On the other hand it does not give a high level of abstraction when it comes to dealing with the threats. The RBIM however gives a model with a higher level of abstraction for dealing with the risk of fraud in the rural banking industry.

9.5 Rural Banking Integrity Model (RBIM)

Having analysed the threats of the rural banking industry, the Rural Banking Integrity Model (RBIM) is presented as an innovative model for dealing with fraud risks. It introduces community based mechanisms for identification and authentication codes based on set of traditional symbols for authentication. It also deals with various issues ranging from managing conflicting tasks to user authentication that could be exploited to commit fraud. It also incorporates the fraud prevention controls into the transaction

process in such a way that members of staff do not have the discretion to abide by it or not.

Also each individual control mechanisms used in the RBIM is a necessary condition to execute part of a transaction. When all the control mechanisms act together they become sufficient for a transaction to be successfully completed.

9.6 Identity Certification and Verification

Identity verification and management was seen as one of the main issues creating risks within the rural banking industry. The community based identity certification is proposed as a solution to this particular problem.

It was shown in chapter two that personal identity is a social construct and with such strong community identity in rural Ghana it becomes natural to use the community as the mean to verify customer identity. The community based identity certification is therefore used in the RBIM as a means to achieve that. In this certification mechanism, certified family or community leaders are used to certify the identities of people thereby staking a family or a trade association's reputation on the certified customer.

9.7 Verification of Authority

It was seen that the main vulnerability that enables fraud is that fact that records cannot be meaningfully tied to the physical person, resource or genuine authorisation that they represent. Also the current mechanism for identifying the identity of a customer and the authority to perform a transaction is a signature but this is thought to have a 0.3 risk of forgery. This is by far higher compared to the 0.001 probability of guessing a traditional four digit numeric PIN is used.

Rural communities being largely illiterate and having their own traditional symbols, the Adinkra system of symbols was used in the RBIM. A 4 code personal identification code/transaction authentication code (PIC/TAC) is used in the RBIM. Using 20 Adinkra symbols the probability of guessing a PIC/TAC correctly reduces to 0.00000625 making it even more secure than the traditional PIN.

Also the Transaction Verification Code (TVC) is proposed as a means of verifying the authenticity of cheques and other source documents.

These mechanisms are all aimed at tying the various components of transactions to each other and removing opportunity for deception.

9.8 Separation of duties (SOD)

Static, dynamic and object based separation of duties are used in the RBIM to deal with conflicts which could lead to fraud risk. In object based SOD the level of conflict should be a function of the previous activity by a particular employee on an account and the current transaction that the employee wants to perform given all other transactions performed on the said account. In the use of object based separation of duty, the level of conflict indicates the level of risk. Hence the measurement of the conflict or risk would be used to indicate the level of authorisation required for the transaction to go through.

9.9 Compliance and Governance

It is clear that the threats faced by organisations directly affect the ability of these organisations to achieve their stated goals. Internal control and the maintenance of security are seen as a strategic activity which ensures that the objectives of an organisation are met.

The implication is that mechanisms that are designed to deal with risks should be aligned with business goals. Most business functions have come to the realisation that the best means achieving success of a strategy largely depend on its alignment with the organisation's environment and culture (Pearce and Robinson, 2000). The environment whether internal or external is always unique and has various characteristics that determine that certain mechanisms work better than others. It also presents various opportunities to the organisation to take advantage of. The environment however also presents some unique threats that must be dealt with.

It is clear, as discussed earlier, that rural banks face many threats, some being unique and others in common with businesses in general and the banking industry in particular. The most important issues issue is not the presence of the threat but rather how the banks respond to these threats. The best way of dealing with issues of such strategic significance is to carve out solutions which take advantage of the environment by aligning the solution with the conditions inherent in the environment. The Rural Banking Integrity Model does exactly that. It takes advantage of the characteristics of the rural banking industry and rural Ghana and design a system that would be able to best secure the business interest and support the achievement of their organisational goals

The key here was to first understand the environment in order to take advantage of it. This enabled choosing a path that allowed building on the industry's capabilities, taking advantages of the opportunities available. It also allowed a strategy to be chosen such that the impact of the risks inherent in the environment and limitations in the organisation are avoided.

9.10 Security and Cultural Considerations

Most often than not systems have been taken from one context and implemented in another without modification. The analysis of the rural banking industries clearly shows that this does not work since many conventional banking practices will not work in the rural banking context. These mechanisms however could work well when they are deployed taking into consideration societal, cultural and other contextual characteristics. Context was shown to be very important and that standards should therefore be modified to suit each system in order to be effective.

9.11 Fraud as a Systemic Issue

Fraud control is often thought to be a very targeted exercise that aims at detecting ongoing frauds or situations that precede frauds. This aims at knowing all the forms of fraud and the events that lead to or enable a person or company being able to profit at the expense of the company providing the service. Some of these models use intrusion detection and audits to detect and control fraud. This thesis looks beyond specific instances of fraud manifestation and adopts the view that fraud occurs as a result of systemic weaknesses that allow the creation of deception and reducing these weaknesses is the best means for controlling fraud. This view is also adopted because it can also deal with unknown fraud instances considering the dynamic diverse nature way that fraud is manifest.

9.12 The Role of Various Actors

This thesis looks differently at actors within the system with regards to security design. It is obvious that actors, either within or outside a system, influence the system with

what they do. The view adopted in this work is not only about what these actors can do to influence the system but rather looks at it at two levels.

The first is the level of control that one has over actors of the system. Internal actors have a high level of knowledge and are close to the system and system managers have a considerable level of control over these actors within a system. On the other hand system managers do not have much control over actors external to the system. They are however not only seen as possible malicious subjects but could be taken advantage of to improve performance of the system.

The second issue is the acknowledgement that the characteristics of the system its actors and its environment offer limitations and or abilities that must be taken advantage of in the process of designing systems to prevent threats. This work clearly shows that characteristics of external factors though system managers have no control can have as much influence and can become a major player in the operation of a security system. The characteristics of rural Ghana are taken advantage of to improve security of rural banks.

9.13 Future Research

Though the questions that this research sought to answer were all thoroughly answered there are some issues that will need to be studied further in the future. These issues are discussed subsequently.

9.13.1 Culture and Security Interactions

There is no doubt that soft issue such as traditions and culture play a role in effectiveness of a security system. Examining the issue of culture and its fusion into technology is a very complex undertaking. This is mainly due to fact that human

behaviour is very unpredictable and sometimes illogical. There is therefore the need to take time to study the subtleties in the subject matter. Further work is also needed to determine the extent to which soft issues affect the effectiveness of security and which factors must come into play in choosing one mechanism over another. The issues that affect the response of people to specific security mechanisms and technologies should be researched further to understand which mechanisms will work better in what societies.

9.13.2 Implementation Model

This research took a variety of mechanisms from various security models and used these mechanisms to develop a model for the rural banking industry. This raises the issue of composability of these mechanisms. It is not very clear that these mechanisms when put together within the context of the rural banking industry would be able deliver the level of security anticipated. It would be very useful to have an implementation model to investigate the issues of composability of any integrity mechanisms and cryptographic algorithms that might be used to implement the RBIM.

9.13.3 Replication of Work

There is the need to replicate the work to cover a greater part of the country to improve the current RBIM. There is the possibility of subcultures that might require slight variation to the designs. Also the northern part of Ghana was not included in the field study and since they are thought to have differences in culture it would be desirable to replicate this study in that region especially in order to incorporate their characteristics. This is desirable because the rural banking industry and the ARB Apex bank cover the whole of the country and the differences in culture must be reflected in the design.

9.13.4 Object based separation of duties

As mentioned earlier object based separation of duty is used in the RBIM to deal with separation of duty problems in the rural industry. Further work however is required to develop a mathematical model for calculating a value which to represent the level of conflict. This value should be such that it can be used to determine what type of access should be given to employees. Achieving this model would greatly support separation of duty and increase the level of granularity in the separation of duties function.

9.14 Conclusion

The research work has added to the understanding of the rural banking industry in Ghana in terms of the fraud risks faced and the possible internal controls that can be used to deal with these risks.

A clear description of the risks associated with the operations of rural banks in Ghana has been done. A comprehensive and coherent system design has been done to deal with the fraud risks of the rural banking industry and if implemented should give assurance that the business processes of the rural banks are safe and secure. This design has introduced innovative developing mechanisms for managing dynamic role based access control and dynamic separation of duties based on the past activities of users is also expected to be developed.

10 References

AL-ZAMANY, Y., et al. (2002) The Cultural Acceptability of the EBEM in Yemen. *Managerial Auditing Journal,* **Vol 17** (9).

ALBERTS, C. J. and DOROFEE, A. J. (2005) *Mission Analysis Assurance Protocol(MAAP); Assesing Risk in Complex Environments.* Carnegie Mellon University. CMU/SEI-2005-TN-032.

ALBRECHT, C. C. and ALBRECHT, W. S. (2006) Strategic Fraud Detection: A technology Based Model.

ALBRECHT, W. S., et al. (2003) *Fraud Examination.* Mason: South Western.

ANDAH, D. O. (2005) Regulation, Supervision and Access to Microfinance Regulation; The case of Ghana. Iris Centre, USA.

ANDAH, D. O. and STEEL, W. F. (2003) *Rural and Microfinance Regulation in Ghana; Implications for Development and Performance of the Industry.* Washington DC, USA: World Bank Group.

ANDERSON, A., et al. (1994) Security modelling for organisations *2nd ACM Conference on Computer and communications security* Fairfax, Virginia, United States ACM Press.

ANDERSON, R., et al. (2001) Security Policies. *Advances in Computers,* **55**.

ANDERSON, R. J. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley and Sons Inc.

ARB APEX BANK (2008) *Rural/Community Banks* ARB Apex Bank, [cited 12 July 2009]. Available from http://www.arbapexbank.com/rcbs.htm.

ARNOLD, M., et al. (2008) How Kerviel exposed lax controls at Société Générale. *Financial TImes.* London, Financial TImes Ltd.

ARROW, K. J. (1964) The Role of Securities in the Uptimum Allocation of Risk-Bearing. *Review of Economic Studies,* **31** (2)**,** 91-96.

ARYEETEY, E. and KWAKYE, E. (2005) *Policy Brief 9.* London: Inter-Regional Inequality Facility-Overseas Development Institute.

ASHENDEN, D. (2008) *Information Security management: A human challenge?* Swindon: Department of Informatics & Sensors, Cranfield University.

ASSOCIATION FOR PAYMENT CLEARING SERVICES (2007) *UK Chip and PIN Report* London: Association for Payment Clearing Services.

AZIZ, B., et al. (2006) Reconfiguring Role Based Access Control Policies Using Risk Semantics.

BANK OF GHANA (2009) *Register of Licensed Rural Banks as at June 2009.* Accra: Bank of Ghana.

BANKING SUPERVISION DIVISION (2005) *Guidelines for Banking Licences: BSD FORM LGBI.1.* Accra: Bank of Ghana.

BANKING SUPERVISION DIVISION (2006) *Guidlines for Rural Banking Licence: BSD FORM LGRB.1.* Accra: Bank of Ghana.

BARKER, W. C. (2003) *Guideline for Identifying an Information System as a National Security System.* Gaithersburg: Computer Security Division, National Institute of Standards and Technology.

BASEL COMMITTEE (1998) *Interal Control Systems in Banking Organisations.* Basel: Bank for International Settlement.

BASEL COMMITTEE ON BANKING SUPERVISION (1998) *Framework for Internal Control System in Banking Organisations.* Basel, Switzerland: Bank for International Settlements.
BASEL COMMITTEE ON BANKING SUPERVISION (2001) *Consultative Document: Operational Risk.* Basel: Bank for international Settlements.
BBC (2006) *Bank Manager in 21 Million Loan Fraud.* British Broadcasting Coporation, [cited 10 November 2008 2008]. Available.
BCBS (2001) *Consultative Document: Operational Risk.* Basel: Bank for international Settlements.
BLAKLEY, B., et al. (2001) Information Security is Information Risk Management. *Workshop on New Security Paradigms.* ACM Press.
BOG (2006) *Guidlines for Rural Banking Licence: BSD FORM LGRB.1.* Accra: Bank of Ghana.
BOND, M. and SKI, P. Z. (2003). *Decimalisation Table Attacks for PIN Cracking*. University of Cambridge.
BOSWORTH, S. and KABAY, M. E. (2002) *Computer Security Handbook.* New York, USA: John Wiley & Sons
BOWEN, P., et al. 2006 *Information Security Handbook: A Guide for Managers.* DEPARTMENT OF COMMERCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. National Institute of Standards and Technology, 800-100.
BOWER, J. B. and SCHLOSSER, R. E. (1965) Internal Control-Its True Nature. *Accounting Review,* (April)**,** 338-344.
BREWER, D. F. C. and NASH, M. J. (1989) The Chinese Wall Security Policy. *IEEE Symposium on Research Security and Privacy.* Oakland Califonia, IEEE.
BRITISH BROADCASTING CORPORATION (2006) *Bank Manager in 21 Million Loan Fraud.* British Broadcasting Coporation, [cited 10 November 2008 2008]. Available.
BRITISH BROADCASTING CORPORATION (2008) Banks Hit Worldwide by US Fraud. Available from http://news.bbc.co.uk/1/hi/business/7783236.stm
BRITISH STANDARDS INSTITUTION (2005) Information Technology-Security Techniques-Code of Practice for Information Security Management British Standards Institution.
CALBOM, L. M. (2002) *Government Purchase Cards; Control Weaknesses Expose Agencies to Fraud and Abuse.* United States General Accounting Office.
CANETTI, R. (2008) Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency. *International Colloquium on Automata, Languages and Programming.* Reykjavik, Iceland, Springer-Verlag.
CARVAJAL, D. and BROTHERS, C. (2008) No hint of glamor or brilliance in former trader's life. *New York Times.* New York, New York Times Company.
CDC CONSULT LIMITED (2009) People Management Challenges of Rural Banks in Ghana. [cited 14 July 2009]. Available from http://cdcconsult.org/articles/?p=13
CIFAS (2009) *Identity Fraud and Identity Theft.* CIFAS, Available from http://www.cifas.org.uk/default.asp?edit_id=561-56.
CISCO (2002) *The Science of Intrusion Detection System Attack Identification.* San Jose: Cisco Systems Inc.
CLARK, A. (2008) The Victim of Bernard Madoff's Fraud. *The Guardian.* London, Guardian News and Media Ltd.

CLARK, D. D. and WILSON, D. R. (1987) A Comparison of Military and Commercial Computer Security Policies. In: *IEEE Symposium on Computer Security and Privacy*. Oakland California: IEEE.
COKER, A. J. (2002). *The Formal Rural Banking Sector in Ghana: An Analysis of the Performance of Rural Banks and the Agricultural Development Bank*. Phd. University of Bradford.
COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISION (1994) Internal Control-Integrated Framework. Jersey City, New Jersey, Commitee of Sponsoring Organisation of the Treadway Commission.
COMMUNITY BANKERS OF WISCONSON (2009) *Community Bank Advantages.* Community Bankers of Wisconson,, [cited 12 July 2009]. Available from http://www.communitybankers.org/about/what-is.php.
COMPTROLLER OF THE CURRENCY ADMINISTRATOR OF NATIONAL BANKS (2001) *Internal Control.* Washington DC: Office of the Comptroller of the Currency, US Treasury Department.
COSO (2005) *Internal Control-Integrated Framework.* Commitee of Sponsoring Organisation of the Treadway Commission, [cited 08/03/06 2006]. Available from http://www.coso.org/publications/executive_summary_integrated_framework.htm.
CRAWFORD, N. and HOPPE, N. 2005 *Dragging Operational Risk Management into the 21st Century*. Business Resilience Group,
CVRCEK, D., et al. (2005) PIN (& Chip) or signature – beating the cheating? In: *Thirteenth International Workshop on Security Protocols.* Cambridge, pp. 69-75.
DEGBEY, J. L. (1997) *African Family Structure.* Japan International Cultural Foundation [cited 16/08/2008 2008]. Available from http://www.jicef.or.jp/wahec/ful217.htm.
DELAC, K. and GRGIC, M. (2004) A Survey of Biometric Recognition Methods. *46th International Symposium Electronics in Marine.* Zadar, Croatia.
DELOITTE DEVELOPMENT LLC (2004) *Antifraud Programs & Controls.* USA: Deloitte & Touche USA LLP.
DEPOSIT ACCOUNT FRAUD COMMITTEE (2000) *Signature Verification Evolution to Exception Check Review.* Washington: American Bankers Association.
DOIG, A. (2006) *Fraud.* (Crime and Society Series) Cullompton: Willan Publishing.
DONZELLI, P. and BRESCIANI, P. (2004) Improving Requirements Engineering by Quality Modelling - A Quality-Based Requirements Engineering Framework. *Journal of Research and Practice in Information Technology,* **36** (4).
E-HARMONY (2009) *The Ghanaian Marriage Ceremony.* e-Harmony, [cited 30/12/2009 Available from http://www.projectwedding.com/biography/list/Ghana_Bride/the-ghanaian-marriage-ceremony.
ECCLES, R., et al. (2001) Risk of Risk. *Balance Sheet,* **9** (3)**,** 28-32.
EDITORIAL COMMITTEE (2005) *Annual Report 2004.* Accra: Bank of Ghana.
EDITORIAL COMMITTEE (2008) *Annual Report 2007.* Accra: Bank of Ghana.
EDITORIAL COMMITTEE (2009) Linking Rural Banks in Ghana. *RBCIP Newsletter.* Accra, Rural Bank Computerisation & Connectivity Project

ESSEL, T. T. and NEWSOME, M. (2000) Effectiveness of Institutional Credit for Rural Development in Africa: A Control Case Study of Rural Banks in Ghana. *Journal of Sustainable Development in Africa,* **2** (1).
FAFINSKI, S. (2005) Identity Theft and the Internet. *BCS Thought Leadership Debate on ID Cards.* British Computer Society.
FARRAIOLO, D. and KUHN, R. (1992) Roles Based Access Controls. *15th National Computer Security Conference.* Baltimore, National Institute of Standards and Technology, Gaithersburg
FEARON, J. D. (1999). *What is Identity (As we use it now)?* University of Stanford.
FLAST, R. H. (2009) *No Excuses: A Business Process Approach to Managing Operational Risk* John Wiley and Sons Ltd.
FOLEY, S. N. (2003) A Non Functional Approach to System Integrity. *IEEE Journal on Selected Areas in Communications,* **Vol. 21** (No 1).
FORE (2005) *Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities* Chicago: AHIMA.
FOUNDATION OF RESEARCH AND EDUCATION (2005) *Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities* Chicago: American Health Information Management Association (AHIMA).
GARCIA-SORDO, J. B. and BAREN, A. W. (1999) National Culture and Preference for Alternate Accounting Controls *International Marketing Review,* **Vol16** (4/5)**,** 314-325.
GENERAL ACCOUNTING OFFICE. 1999 *Standards in Internal Control in the Federal Government.* UNITED STATES GENERAL ACCOUNTONG OFFICE. United States Federal Government,
GENERAL ACCOUNTING OFFICE. 2002 *Government Purchase Cards; Control Weaknesses Expose Agencies to Fraud and Abuse - Statement of Linda M. Calbom.* United States General Accounting Office,
GERBA, M. and SOLMS, R. V. (2005) Management of Risk in the Information Age. *Computers and Security,* **24** (1)**,** 16-30.
GHANA NEWS AGENCY (2008) *Tailor with double ID remanded.* [cited 03/12/2008 Available from http://news.myjoyonline.com/news/200812/23481.asp.
GHANA STATISTICAL SERVICES (2005) *Ghana in Figures.* Accra: Ghana Statistical Service.
GHANAIAN TIMES (2008) *Man caught with 3 voter IDs.* [cited 04/12/2008 Available from http://news.myjoyonline.com/news/200812/23512.asp.
GOCKING, R. (2005) *The History of Ghana.* Greenwood Press.
GOGUEN, J. A. and MESEGUER, J. (1982) Security Policies and Security Models. *Symposium on Security and Privacy.* Los Alamitos, IEEE Computer Society Press.
GRANT, I. (2007) Identity Management: The Expert View. *http://www.computerweekly.com.* Sutton Surrey, Reed Business Information Ltd.
HALEY, C. B., et al. (2004) Deriving security requirements from crosscutting threat descriptions *Proceedings of the 3rd international conference on Aspect-oriented software development* Lancaster, UK ACM Press.
HALEY, C. B., et al. (2002) Using Trust Assumptions in Security Requirements Engineering. *iTrust Workshop*

HALEY, C. B., et al. (2006) Using Trust Assumptions in Security Requirements Engineering. *Requirements Engineering Journal,* **Vol. 11** (No. 2)**,** pp.138-151.
HARDING, L. (2004) Secretary Guilty of £4 Million Fraud. *Mail on Sunday.* London, Associated Newspapers Ltd.
HAUBENSTOCK, M. (2001) The Evolving Operational Risk Management Framework. *RMA Journal,* **December 2001**.
HEAD, R. V. (1966) The banking information system concept *Communication of the ACM,* **9** (7)**,** 491-496
HENDERSON, L. (2000) *Bank and Banking Related Fraud.* Crimes of Persuasion, [cited 13 August 2009]. Available from http://www.crimes-of-persuasion.com/Crimes/Business/bank_fraud.htm.
HERNDON, P. (2009) *Family Life Among the Ashanti of West Africa.* [cited 20 September 2009 Available from http://www.yale.edu/ynhti/curriculum/units/1991/2/91.02.04.x.html.
HILDER, T. (1995) *The Viable System Model.* Cavendish Software Ltd.
HILLSON, D. (1999) Developing Effective Risk Responses. *Annual Project Management Institute Seminars and Symposium.* Philadelphia.
HOFSTEDE, G. (1980) *Culture's Consequences: International Differences in Work-Related Values.* Beverly Hills, CA: Sage Publications.
HOLTON, G. (1996) *Barings Debacle.* Contingency Analysis, [cited 5/01/2010 Available from http://www.riskglossary.com/link/barings_debacle.htm.
HOLTON, G. A. (2004) Defining Risk. *Financial Analysts Journal,* **60** (6)**,** 19-25.
HU, V. C., et al. (2006) *Assessment of Access Control Systems* Gaithersburg: Computer Security Division, National Institute of Standards and Technology.
IFAD (2007) *Ghana Statistics.* International Fund for Agricultural Development, [cited 22/08/2008 2008]. Available from http://www.ruralpovertyportal.org/english/regions/africa/gha/statistics.htm.
INDEPENDENT COMMUNITY BANKERS OF AMERICA (2009) *Community Bank Advantages.* Independent Community Bankers of America, [cited 12 July 2009]. Available from http://www.icba.org/communitybanking/index.cfm?ItemNumber=556&sn.ItemNumber=1744.
INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE (2005) COBIT 4.0. Rolling Meadows, Illinois, Information Technology Governance Institute.
JACKSON, S. and PHILIP, G. (2010) A Techno-cultural Emergence Perspective on the Management of Techno-change. *International Journal of Information Management*.
JAMESON, J. (1998) Playing the Name Game. *Risk,* **10** (11)**,** 38-42.
JHA, A., et al. (2004) *Ghana Microfinance Investment Environment Profile.* New Jersey: Princeton University.
JOHNSTONE, D. and WONG, E. C. Y. (2008) Practicing Information Technology Auditing for Fraud. *Information Systems Control Journal,* **Vol 1**.
JONSSON, E. (1998) An Integrated Framework for Security and Dependability. In: *New Security Paradigm Workshop.* Charlottesville, Virginia, USA: ACM, pp. 22-29.
JØSANG, A., et al. (2006) A Method for Access Authorisation Through Delegation Networks. *Fourth Australasian Information Security Workshop.* Hobart, Australia.
KARYDA, M., et al. (2005) Information Systems Security Policies: A Contextual Perspective. *Computers & Security,* **Vol 24** (3)**,** 246-260.

KHUN, D. R., et al. (2001) *Introduction to Public Key Technology and the Federal PKI Infrastructure.* National Institute of Standards and Technology.
KING, J. L. (1998) Defining Operational Risk. *Algo Research Quarterly,* **Vol 1** (2)**,** 37-42.
KPMG (1999) *Internal Control: A Practical Guide.* (The KPMG Review) Service Point (UK) Ltd.
KPMG (2007) *Profile of a Fraudster.* Switzerland: KPMG Holding.
KUHN, D. R., et al. (2002) Cost Effective Use of Formal Methods in Verification and Validation. *Foundation 02: A V&V Worskshop.* Laurel, Maryland, USA, US Dept of Defence.
KUHN, D. R., et al. (2003) Practical Application of Formal Methods in Modelling and Simulation. *Summer Computer Simulation Conference.* Montreal, Canada.
KUMAR, S. (1995). *Classification and Detection of Computer Intrusions*. PhD. Purdue University.
KVARNSTROM, H., et al. (2000) Combining Fraud and Intrusion Detection- Meeting New Requirements. *Fifth Nordic Workshop on Secure IT Systems (NorSec 2000).* Reykjavik, Iceland,.
LANZA, R. B. (2003) *Proactively Detecting Occupational Fraud Using Audit Reports.* Altamonte Springs Institute of Internal-Auditors Research Foundation
LIN, T. Y. (1989) Chinese Wall Security Policy - An Aggressive Model. *Fifth Annual Computer Security Applications Conference.* Tuscon, Arizona.
LISTER, D. (2006) 2004: Bank Manger of the Year. 2006: Guilty of £21 Million Bank fraud *The Times.* London, News International Ltd.
LOOCK, M. and ELOFF, J. H. P. (2005) Investigating the Usage of the Chinese Wall Security Policy Model for Data Mining. *International Symposium on Information and Communications Technologies.* Cape Town.
LOWRY, J. S. (2003) The Identification Process Deconstructed. *NIST Smart Card Workshop.* National Institute of Standards and Technology.
LUO, X., et al. (2009) The Impact of National Culture on Workplace Privacy Expectations in the Context of Information Security Assurance. *Americas Conference on Information Systems.* San Francisco, California.
MAINELLI, M. (2002) Industrial Strengths: Operation Risks and Banks. *Balance Sheet,* **10** (2)**,** 25-35.
MCCALLISTER, E., et al. (2009) *Guide to Protecting the Confidentiality of Personally Identifiable Information* Gaithersburg: Computer Security Division-National Institute of Standards and Technology.
MCLAUGHLIN, J. L. and OWUSU-ANSAH, D. 1994 *A Country Study: Ghana - Historical Setting.* FEDERAL RESEARCH DIVISION. Library of Congress (DT510.G44 1995).
MCLEAN, J. (1982) A Comment on the Basic Security Theorem of Bell and La Padula. *Information Processing Letters,* **20** (2).
MENEZES, A. J., et al. (2001) *Handbook of Applied Cryptography.* CRC Press.
MINSKY, N. H. and UNGUREANU, V. (1998) Unified Support for Heterogeneous Security Policies in Distributed Systems. *USENIX Security Symposium.* San Antonio.
NASH, M. J. and POLAND, K. R. (1990) Some Conundrums Concerning Separation of Duty. *IEEE Symposium on Research in Security and Privacy.* Oakland California, IEEE.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2004) *Standards for Security Categorization of Federal Information and Information Systems*

Gaithersburg: Computer Security Division, National Institute of Standards and Technology.
NIEKERK, J. F. V. and SOLMS, R. V. (2009) Information security culture: A management perspective. *Computers & Security*.
O'GARA, J. D. (2004) *Corporate Fraud: Case Studies in Detection and Prevention.* West Sussex: John Wiley & Sons Inc.
OFFEN, R. (2002) Domain understanding is the key to success system development, Requirements Engineering. *Springer Verlag* **7**(3).
OFFICE OF THE CORPORATE CHIEF INFORMATION OFFICER (2003) *Identity Authentication and Authorisation in Electronic Service Delivery.* Ontario: Management Board Secretariat - Government of Ontario

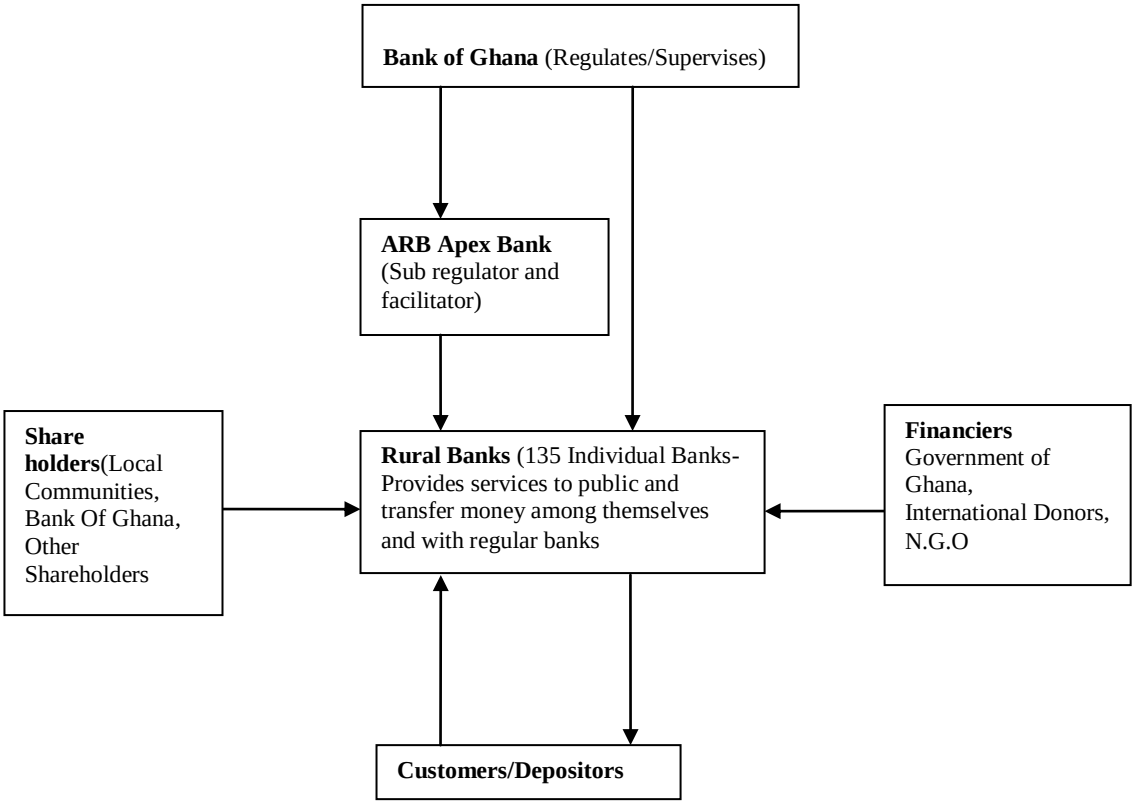
OFFICE, S. F. (2003) *Philip Ashley Jailed for Defrauding Bank in £3.7 Million Loan Deals* Serious Fraud Office, 2009]. Available from http://www.sfo.gov.uk/news/prout/pr_190.asp?id=190.
ORGILL, G. L., et al. (2004) The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems *5th conference on Information technology education* Salt Lake City, UT, USA ACM Press.
OWEN, S. (1998) *Information Security management; An Intrduction.* British Standards Institue.
OWUSU-ANSAH, D. 1994 *A Country Study: Ghana - Society and Its Environment.* FEDERAL RESEARCH DIVISION. Library of Congress (DT510.G44 1995).
OXFORD UNIVERSITY PRESS (2002) Oxford English Dictionary. In: SOANES, C. (Ed.) Oxford, Oxford University Press.
PATHAK, J. (2005) Risk Management, Internal Controls and Organizational Vulnerabilities. *Managerial Auditing Journal,* **20** (6).
PEARCE, J. A. and ROBINSON, R. (2000) *Formulation Implementation and Control of Competitive Strategy* McGraw-Hill Higher Education.
PELTIER, T. R. (2006) Social Engineering: Concepts and Solutions. *EDPACS, Reston,* **Vol 33** (8)**,** 1-13.
PERELSON, S. (2001). *SoDA: A Model for the Administration of Separation of Duty Requirements in Workflow Systems*. **Port Elizabeth Technikon**.
PERELSON, S., et al. (2001) Separation of Duty Adminstration. *South African Computer Journal*, **Number 27,** 64-69http://www.nmmu.ac.za/rbotha/Pubs/docs/JP_004.pdf.
PERELSON, S. and BOTHA, R. A. (2000) Conflict Analysis as a Means of Enforcing Statis Separation of Duty Requirements in Worflow Environments. *South African Computer Journal*, **26**.
PIDD, M. (2004) *Systems Modelling; Theory and Practice* West Sussex: John Wiley and Sons Ltd.
POLICE COMMISSIONERS' CONFERENCE-ELECTRONIC CRIME STEERING COMMITTEE (2003) Australasian Identity Crime Policing Strategy. Payneham, Australasian Centre for Policing Research.
PRICEWWATERHOUSECOOPERS (2004) *Information Security Breaches Survey 2004; Identity Management.* London: Department for Trade and Industry.
RAMAGE, S. (2005) *Serious Fraud and Current Issues.* Bloomington: Iuniverse.com.
SALM, S. J. and FALOLA, T. (2002) *Culture and Customs of Ghana.* (Culture and Customs of Africa) Westport, CT: Greenwood Press.
SALTZER, J. H. and SCHROEDER, M. D. (1974) The Protection of Information in Computer Systems. *Communications of the ACM,* **17** (7).

SAMPSON, D. (1999) *Understanding Internal Control.* University of California, Available from http://www.ucop.edu/ctlacct/under-ic.pdf.
SANDHU, R. S. (1992) A Lattice Interpretation of the Chinese Wall Policy. *15th NIST-NCSC National Security Conference.* Baltimore.
SANDHU, R. S. (1993) Lattice Based Access Control Models. *IEEE Computer,* **26** (11)**,** 9-19.
SCHNEIER, B. (2000) *Secret and Lies; Digital Security in a Networked World.* New York: John Riley & sons, Inc.
SCHNEIER, B. (2005a) *Mitigating Identity Theft.* [cited 27 October 2009 Available from http://www.schneier.com/blog/archives/2005/04/mitigating_iden.html.
SCHNEIER, B. (2005b) *Terrorists Don't Do Movie Plots.* Condé Nast Digital, [cited 17 October 2009 Available from http://www.wired.com/politics/security/commentary/securitymatters/2005/09/68789.
SCHNEIER, B. (2006) *Beyond Fear.* USA: Copernicum Books.
SHABUDIN, E. (2007) An Operational Risk Framework. *RMA Journal,* **June 2007**.
SIMON, R. T. and ZURKO, M. E. (1997) Separation of Duty in Role-Based Environments. *10th Computer Security Foundations Workshop*
SMALL, M. (2004) Business and Technical motivation for Identity Management. *Science Direct*, **9** (1)**,** 6-21.
STAJANO, F. and WILSON, P. (2009) *Understanding Scam Victims: Seven Principles for Systems Security.* Cambridge: University of Cambridge Computer Laboratories. No 754.
STEWART, J. M., et al. (2005) *CISSP: Certified Information Systems Security Professional Study Guide.* San Francisco: John Wiley and Sons Inc.
STONEBURNER, G., et al. (2002) *Risk Management Guide for Information Technology Systems.* Gaithersburg: Computer Security Division, National Institute of Standards and Technology.
SUTHERLAND, D. (1986) A Model of Information. *9th National Security Conference.* Gaithersburg.
SWANSON, M. and GUTTMAN, B. 1996 *Generally Accepted Principles and Practices for Securing Information Technology Systems.* DEPARTMENT OF COMMERCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. National Institute of Standards and Technology,
TAYLOR, C. (2006) The RMA Operational RIsk Management Framework. *RMA Journal,* **December 2006**.
THE ADVANCED MEASUREMENT APPROACHED GROUP (2008) *Business Environment and Internal Control Factors.* Philidelphia: Risk Management Association.
THE FRAUD PRACTICE (2008a) *Check Verification.* The Fraud Practice LLC, [cited 29 August 2009]. Available from http://www.fraudpractice.com/FL-Checkverify.html.
THE FRAUD PRACTICE (2008b) *Credit Card Bin Checks.* The Fraud Practice LLC, [cited 12 August 2009]. Available from http://www.fraudpractice.com/FL-binCC.html.
THE FRAUD PRACTICE (2008c) *Real Time Authorisations.* The Fraud Practice LLC, [cited 16 August 2009]. Available from http://www.fraudpractice.com/FL-AuthRealtime.html.
THIRLWELL, J. (2002) Operational Risk: The Banks and the Regulators Struggle. *Balance Sheet* **10** (2)**,** 28-31.

TUNG-CHIEN, W. (1987) Some Problems Arisin out of the Cross-Disciplinary Nature of Information System Security. *SIGCPR Computer Pers.,* **11,** 16-27.
TURNBULL, J. (2004) A hard time for soft issues? *The Chemical Engineer,* **Dec 04,** 22-23.
UBINK, J. M. (2007) Between Customs and State Law: Land Management in Peri-Urban Kumasi, Ghana. *Africa-Europe Group for Interdisciplinary Studies.* Leiden.
UK CARD ASSOCIATION (2009) *Transaction Processing.* The UK Card Association, [cited 16 August 2009]. Available from http://www.retailersandcards.org.uk/accept_cards/transaction_processing.html.
UTLEY, I. (2009) *The Essential Guide to Customs & Culture: Ghana.* London: Kuperard.
VEIGA, A. D. and ELOFF, J. H. P. (2010) A Framework and Assessment Instrument for Information Security Culture. *Computers & Security,* **29** (2)**,** 196-207.
WALLACE, J., et al. (2008) The Credit Crunch: a Domino Effect. *Business Perspectives,* **Winter-Spring 2008**.
WEISE, J. (2001) *Public Key Infrastructure Overview.* San Antonio: Sun Microsystems Inc.
WGCB (2001) *Customer due diligence for banks.* Basel: Bank for International Settlements.
WIESMAIER, A., et al. (2005) Outflanking and Securely Using the PIN/TAN *International Conference on Security and Management.* Las Vegas, Nevada.
WILSON, P. (2005) Risk control: A technical view. *Computer Fraud & Security,* **2005** (5)**,** 8-11.
WORKING GROUP ON CROSSBORDER BANKING (2001) *Customer due diligence for banks.* Basel: Bank for International Settlements.
YEBOAH, E. H. (2007) Microfinance in Rural Ghana: Towards an Integrative Approach. In: *Graduate Research Conference on Social Sciences and Management.* Bradford: University of Bradford.

11 Appendices

APPENDIX A: Structure of the rural banking industry



APPENDIX B: Questionnaire – Rural Banks

This questionnaire is part of a PhD research project to help develop a computer security system for the rural banking sector. I would like to mention here that your identity or your banks identity is not required in the study and hence would not be mentioned in any part of the study. Also any information provided would be for academic purposes only and would be treated with utmost confidentiality.

Could you please answer the questions below?

1. How many agencies does your bank have
   ……

2. How many members of staff does your bank have
   A) Full time…….
   B) Part time…….

3. Can you provide an organizational chart or alternatively fill the attached table with the current staff positions (e.g. Manager or clerk) and show their immediate supervisor and their role/function (e.g. counter clerk) within the bank;

a.) Head Office

Authority level	**Supervisor (reports to)**	**Description of role and duties within bank (e.g. Customer services, account opening e.t.c)**
Supervising manager		
Manager		
Supervising accountant		
Accountant		

Projects officer		
Cust. Serv. officer		
Operations Officer		
Clerk		
Clerk		
Other		
Other		

b.) Agency

Authority level	**Supervisor (reports to)**	**Description of role and duties within bank (e.g. Customer services, account opening e.t.c)**
Agency Manager		
Accountant		
Operations Officer		
Clerk		
Clerk		
Other		
Other		

4. How do you deal with the job functions for any position if they become vacant or an employee has to take a leave or some time off?

   ……

   ……

5. Do you do job scheduling and rotation for your staff Yes ( ) No ( )

If the answer to question 5 is yes then answer questions 6, 7 and 8 if not please proceed to question 9

6. What are the objectives for doing job scheduling and rotation
   ……
   ……
   ……

7. At what intervals do you revise your job schedules or rotate jobs?
   ……

8. What are the job roles that are distributed among staff in the job schedule?
   .....
   .....
   .....

9. Is it possible for a member of staff to perform an activity on behalf of the bank other than the ones stated in their job schedule? Yes ( ) No ( )

10. If the answer to question 9 is yes, who would give authorization to the staff to perform that activity?
    …….

11. If a member of staff performs an activity without authorization are there mechanisms to detect it? Yes ( ) No ( )

12. If the answer to question 11 is yes, what are the ways that your bank uses to detect such instances?
    a) ……
    b)……
    c) ……...
    d) ……...
    e) ……..

13. Does your bank have specific procedures/guidelines for delivering your products and services? Yes ( ) No ( )

14. What services does your bank provide to the public? (Please tick)
    a) Savings Account ( )
    b) Current Accounts ( )
    c) Apexlink local Money Transfer ( )
    d) Efie ne fie ( )
    e) Fixed deposit ( )
    f) Call Accounts ( )
    g) Loans ( )
    i) Other ……

15. Please enumerate the processes that your bank goes through to deliver the various services mentioned in question 14 in the attached table and the corresponding staff position that performs each stage.

16. Do you have problems in adhering to your processes and or Apex Bank Guidelines for delivering services to the public? Yes ( ) No ( )

17. If the answer to question 16 is yes how you rate the problems you encounter in ensuring that your procedures are adhered to (please circle your answer). **1 2 3 4 5** (where 5 is the highest)

18. What are the sources of the problems you have in adhering to your procedures? Staff ( ) Customers ( ) Management ( ) Apex Bank ( ) (note; you can select more than one group)

19. How do you identify new customers who come to open accounts?
    ……...
20. When a customer comes to perform a transaction in your bank how do you identify him/her?
    ……
    ……

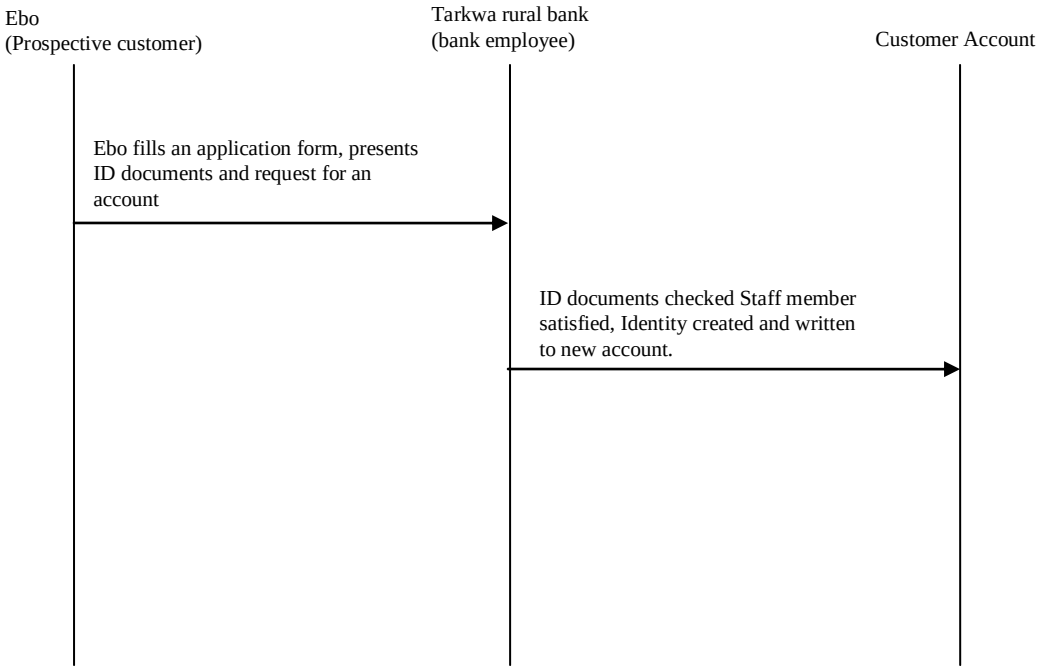
APPENDIX C: Current Banking Processes

I. Apex money transfer process

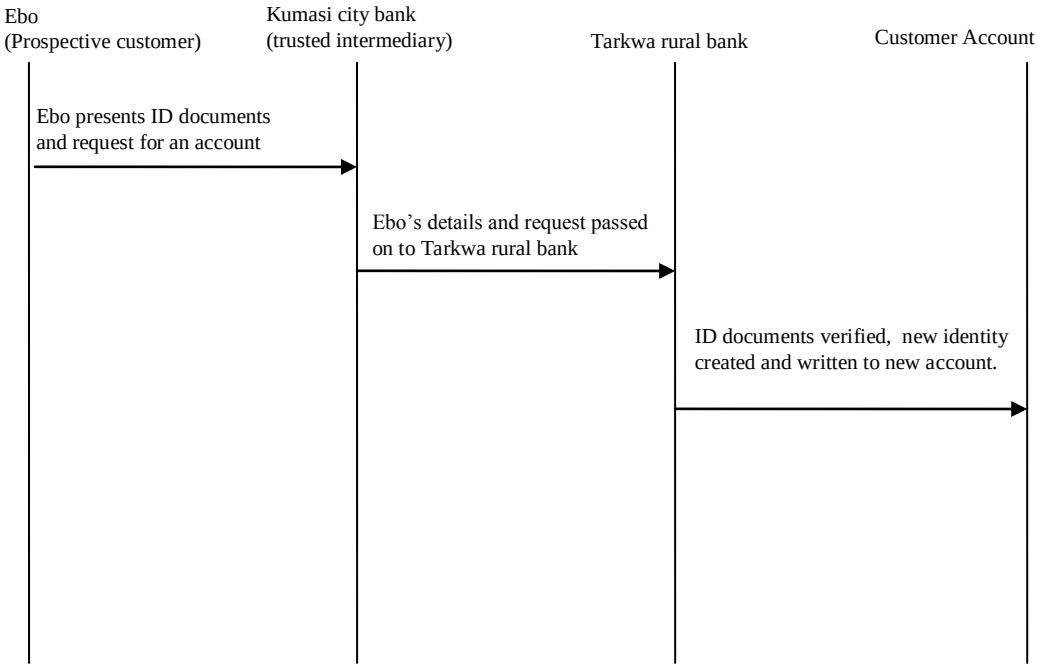
1. Customer request for transfer of money.
2. Details are checked by the clerk and verified by an officer.
3. Customer account is debited or pays in cash to teller.
4. Message is composed on form BO22 and given a MIN.
5. The message is written and recorded in a dispatch book .
6. The message is coded independently by two officers using a test key and prefixed to the message.
7. Message is relayed by electronic means and entered in the outward transfer register.
8. Message is typed onto form BO25 and signed by the two officers who coded the message and part one sent to the paying bank, part two sent together with an interApex/RCB credit advice form BO27 to the zonal clearing centre and part 3 retained.
9. Message received decoded and authenticated.
10. Message entered in receipt book.
11. Transmitted message to the paying bank and transfer of a fully completed BO27 attached to part 3 of the BO23 form.
12. Preparation of the BO24 form by Apex link clerk and transfer to the Teller.
13. Customer identified by ID payment made.
14. Money is paid to recipient in cash or into the designated account.

ACCOUNT OPENING

II. Identity Verification in Account Opening Process at account holding bank

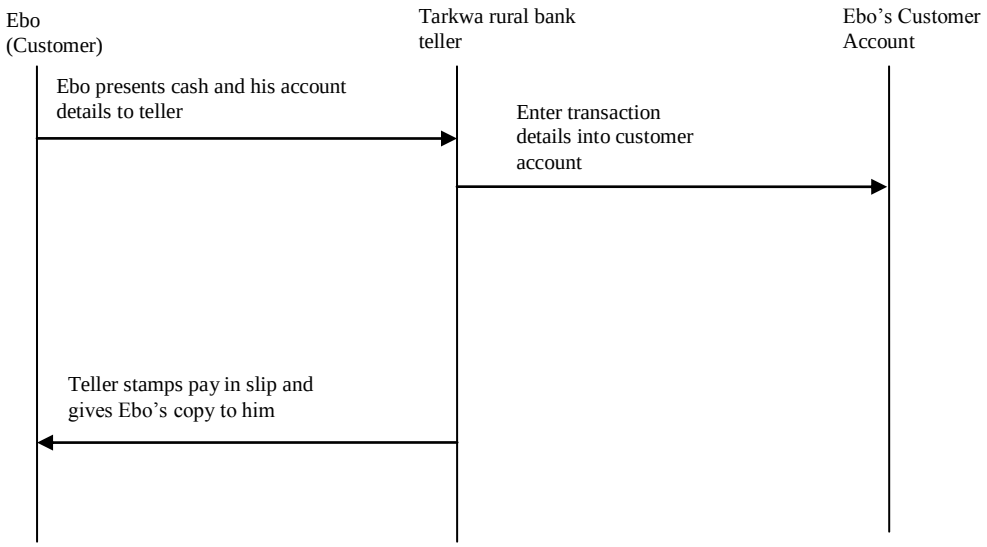


III. **Identity Verification and Account Opening Process from a different bank**

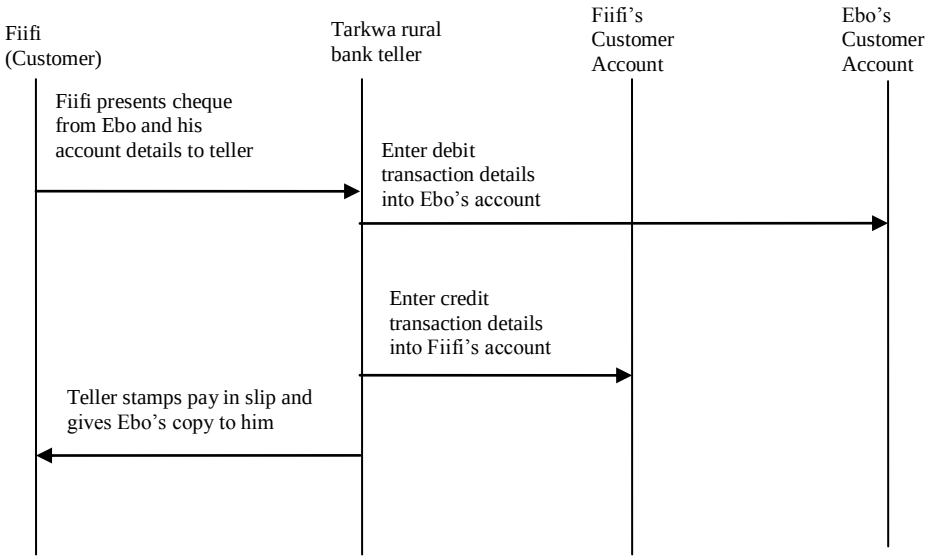


ACCOUNT TRANSACTIONS

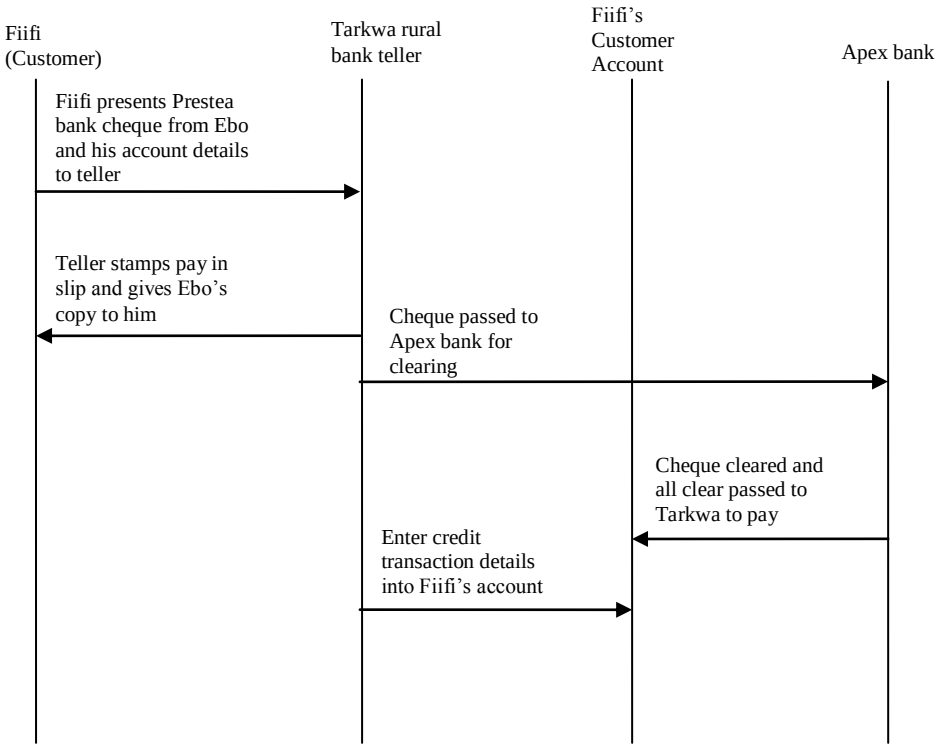
IV. Paying into account



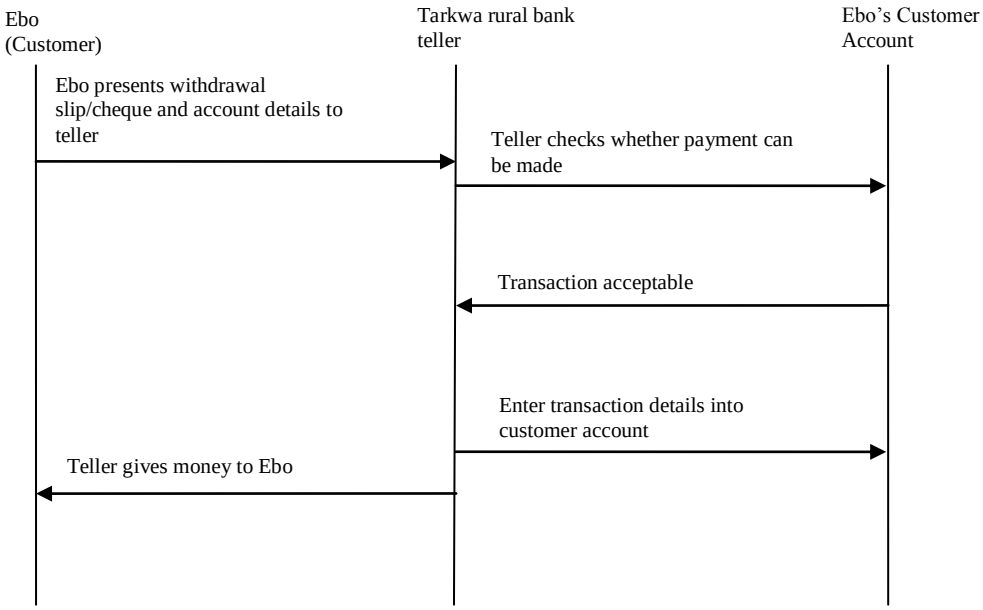
V. Third party cheque payment from same bank



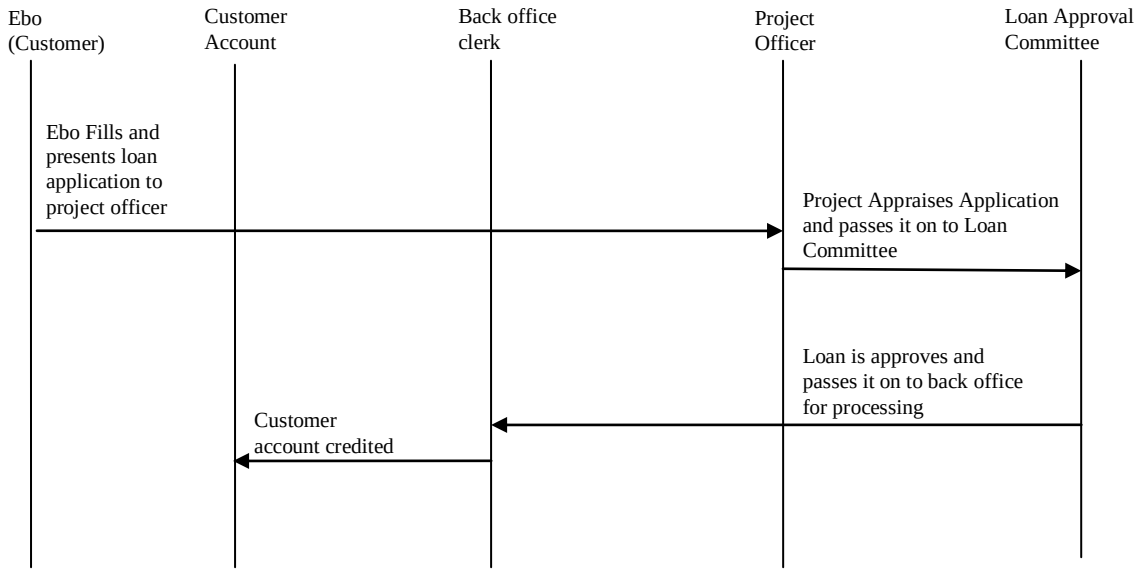
VI. Account to Account transfer/payment from different bank



VII. Withdrawal from account



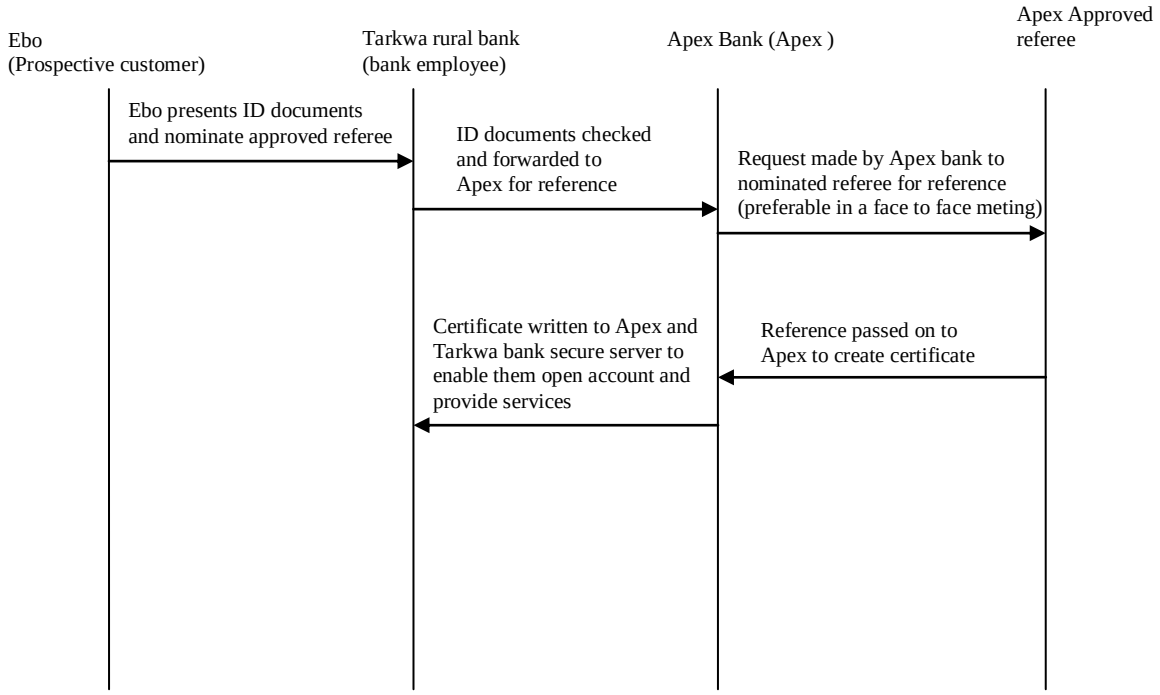
VIII. Loan Application Process



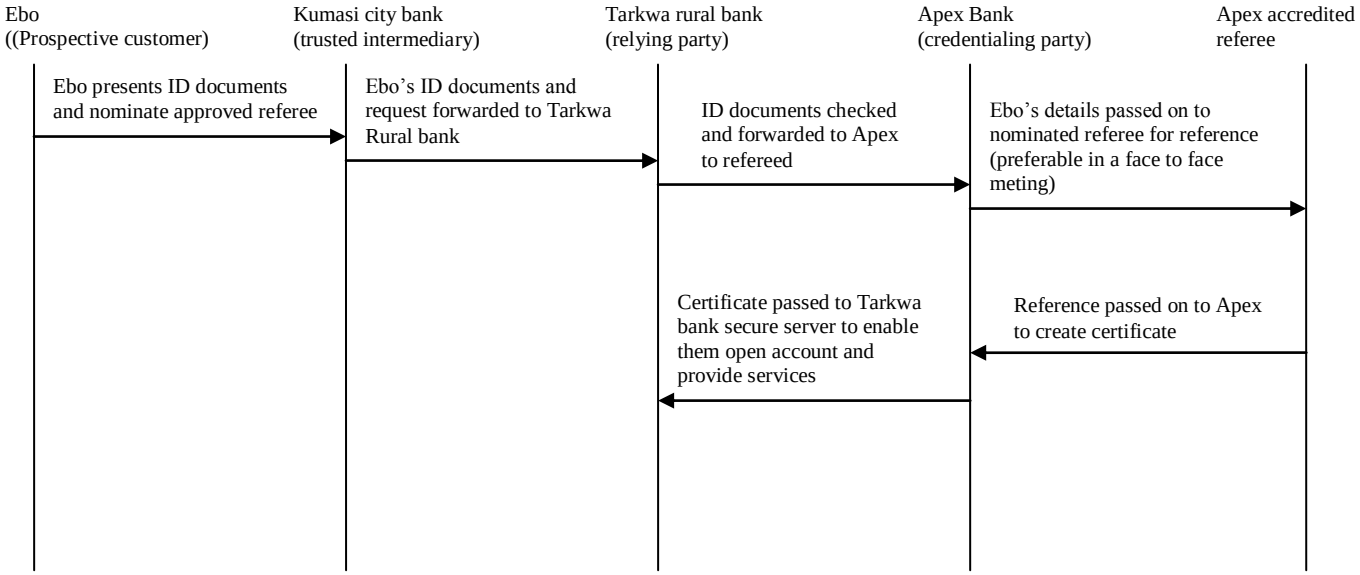
APPENDIX D: Rural Banking Integrity Model Processes

IDENTITY VERIFICATION

I. Identity Verification in Account Opening Process at account holding bank

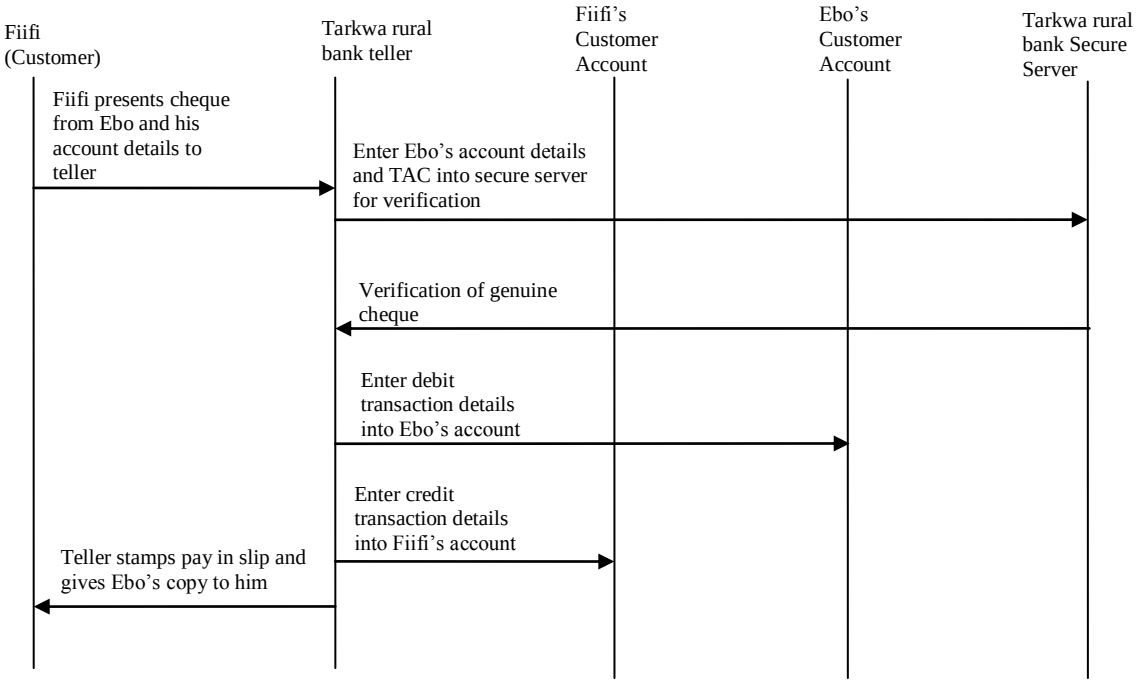


II. Account opening from the city based bank – Efie ne fie

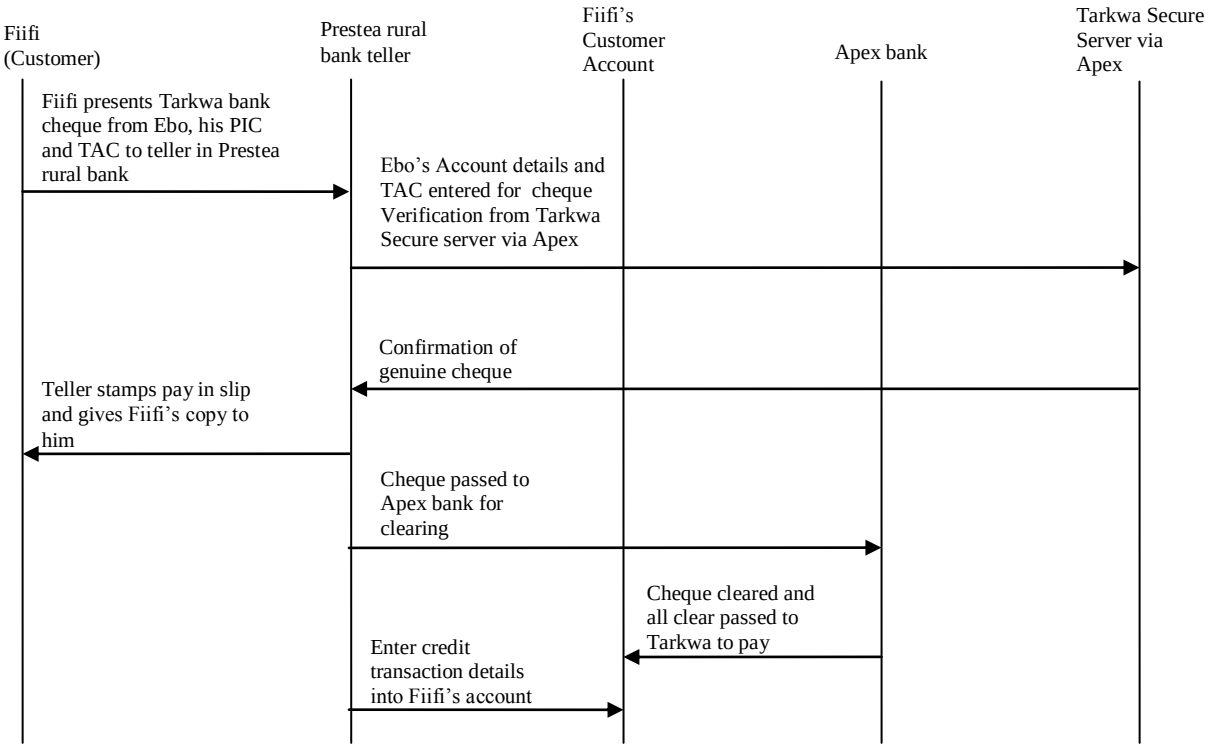


ACCOUNT TRANSACTIONS

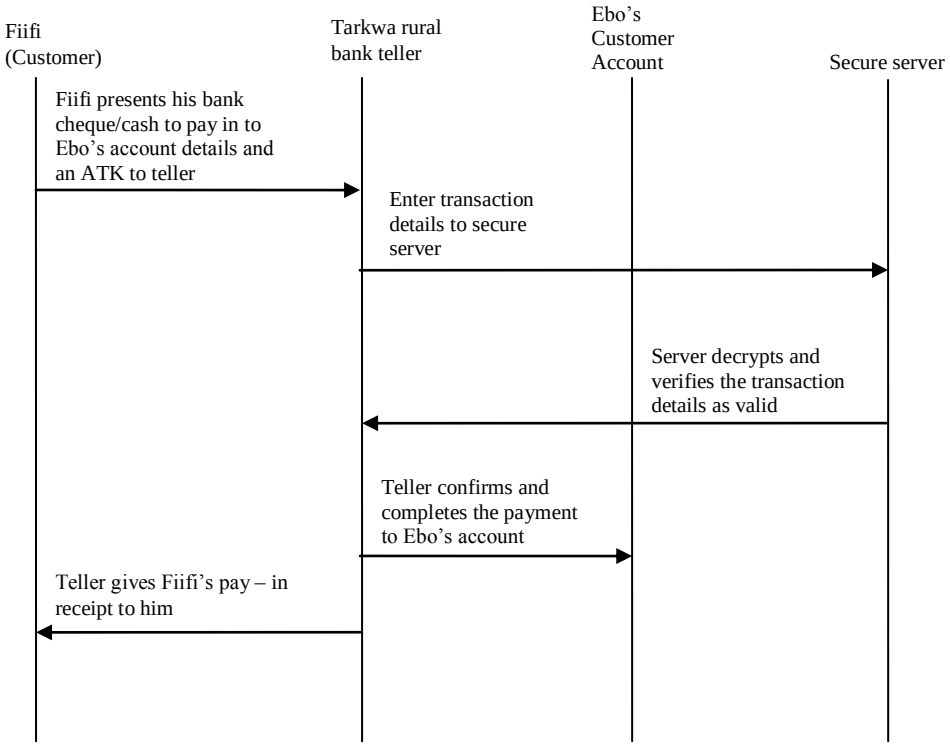
III. Third party cheque payment from same bank and use of TAC



IV. Account to Account transfer/payment from different bank TAC



V. Paying into different customer account and TVC



APPENDIX E: Scenarios Testing

Fraud Type	Variation	Fraud enabling steps	Solution Mechanism
1. Unauthorised withdrawal	A	fraudulent origin of transaction request	Transaction Verification Code
	B	fraudulent origin of transaction request	Transaction Verification Code
2. Unauthorised Loan	A	Non presence of cheque/voucher and ID	Transaction Verification Code Transaction Authentication Code
	B	Non presence of cheque/voucher and ID	Transaction Verification Code Transaction Authentication Code
3. Same day reversal	A	Poor verification of authenticity of reversal	Atomicity transactions, Transaction Verification Code
	B	Poor verification of authenticity of reversal	Atomicity transactions, Transaction Verification Code
4. Job rotation	A	Poor identity verification in a/c opening	Object based separation of duties, Community Based ID Certification
	B	Poor identity verification in a/c opening	Object based separation of duties, Community Based ID Certification
	C	Poor identity verification in a/c opening	Object based separation of duties, Community Based ID Certification
	D	Poor identity verification in a/c opening	Object based separation of duties, Community Based ID Certification
5. False cheque book request	A	Fraudulent origin of request	Transaction Authentication Code
	B	Fraudulent origin of request	Transaction Authentication Code
6. Signatory alteration	A	Fraudulent origin of request	Object based separation of duties, TAC
7. Money transfer	A	Non secure transfer of transaction details	Transaction Authentication Code

Fraud Type	Variation	Fraud enabling steps	Solution Mechanism
8. Account opening	A	Initial paying in of deposit	Atomicity
	B	Lack of linkage of a/c opening and pay in	Atomicity
9. Systems admin login	A	Conflict of duty	Static separation of duties
10. Dividend payment	A	Lack of linkage of a/c details and payment request	Account Transfer Key
11. Suspense account	A	delay in transaction completion, unauthorised account transaction	Account Transfer Key
	B	delay in transaction completion, unauthorised account transaction	Account Transfer Key
	C	delay in transaction completion, unauthorised account transaction	Account Transfer Key
	D	delay in transaction completion, unauthorised account transaction	Account Transfer Key
12. Teller till	A	Lack of separation of duties	Static separation of duties
13. Cheque kiting	A	Lack of cross checking	Atomic transaction
14. Account opening with false ID	A	Non reliability of ID document	Community Based ID Certification
	B	Non reliability of ID document	Community Based ID Certification
	C	Non reliability of ID document	Community Based ID Certification
15. Employee ID	A	Poor due diligence	Community Based ID Certification
	B	Poor due diligence	Community Based ID Certification
	C	Poor due diligence	Community Based ID Certification
16. Cheque Fraud 1	A	Lack of detection forged cheque	Transaction Verification Code
	B	Lack of detection forged cheque	Transaction Verification Code
	C	Lack of detection forged cheque	Transaction Verification Code

Fraud Type	Variation	Fraud enabling steps	Solution Mechanism
17. Cheque Fraud 2	A	lack of verification of authorisation of a/c holder	Transaction Authentication Code
	B	lack of verification of authorisation of a/c holder	Transaction Authentication Code
	C	lack of verification of authorisation of a/c holder	Transaction Authentication Code
	D	Lack of detection forged cheque	Transaction Verification Code
18. Cheque Fraud 3	A	lack of verification of authorisation of a/c holder	Transaction Authentication Code
	B	Lack of detection forged cheque	Transaction Verification Code
19. Cheque Fraud 4	A	Inability to verify of Customer wrote amount	Not Solved
	B	lack of verification of authorisation of a/c holder	Transaction Authentication Code
	C	lack of verification of authorisation of a/c holder	Transaction Authentication Code
20. Customer Repudiation	A	Lack of proof of ID of person requesting transaction	Transaction Verification Code

APPENDIX F: Adinkra Symbols