Addis Ababa University

College of Business and Economics

School of Commerce

Department of Project Management

Evaluation of the role of NG|Screener Project on Fraud Prevention: The Case of Commercial Bank of Ethiopia

By:

Melese Gessese

A Research Project Submitted to Addis Ababa University School of Commerce in Partial Fulfillment of the Requirement for the Master of Arts Degree in Project Management

Advisor: Dr. Mengistu Bogale

June 2022

Addis Ababa, Ethiopia

Addis Ababa, Ethiopia

Addis Ababa University

College of Business and Economics

School of Commerce

Department of Project Management

Evaluation of the role of NG|Screener Project on Fraud Prevention: The Case of Commercial Bank of Ethiopia

By: Melese Gessese

Approved By:

Advisor: ---------- Signature ----------Date ----------

Internal Examiner: ---------- Signature---------- Date ----------

External Examiner: ---------- Signature----------Date ----------

DECLARATION

I declare that the research project work entitled “EVALUATION OF THE ROLE OF NG|SCREENER PROJECT ON FRAUD PREVENTION: THE CASE OF COMMERCIAL BANK OF ETHIOPIA” is my original work. This work has not been presented for any other university and is not concurrently submitted in candidature of any other degree, and that all sources of material used for the thesis have been duly acknowledged.

Melese Gessese Signature_____ Date_____

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

CERTIFICATE

This is to certify that this project work, " EVALUATION OF THE ROLE OF NG|SCREENER PROJECT ON FRAUD PREVENTION: The case of Commercial bank of Ethiopia" undertaken by Melese Gessese in Partial fulfillment of the award of Master's degree in Project Management at Addis Ababa University graduate school, is an Original work and not submitted earlier for any degree either at this or any other University.

Advisor: Mengistu Bogale (PhD) Signature_____

Date _____

ACKNOWLEDGMENTS

First of all, thanks of God who gifted me with this wonderful life and helping me in my study and project work, and I would like to express my appreciation to my advisor, Mengistu Bogale (PhD) ,for his advice to do this project work. I would also like to express my gratitude to CBE staffs and all other participants for their cooperation in conducting the study area. Last but not least, I would like to express my deepest gratitude and unreserved thanks to my family and friends for their support of my study.

Contents

List of Tables

List of Figures

ACRONYMS/ABBRIVATION

CBE	Commercial Bank of Ethiopia
CIMA	Chartered Institute of Management Accountants
KPMG	Klynveld Peat Marwick Goerdeler.
ACFE	Association of Certified Fraud Examiners
COSO	Committee of Sponsoring Organizations of the Treadway Commission
IIA	Institute of Internal Auditors
NG	Netguardians
EFCC	Economic and Financial Crime Commission
ICT	Information and Communications Technology
GBAD	Graph-based anomaly detection
ICF	Internal Control framework
IT	Information Technology
ICS	Internal Control System
SD	Standard deviation

Abstract

In the current modern dynamic world, fraud risks become very complex and have been completely challenged by fraudsters to integrate themselves impact into every aspect of the banking and any other organization. Business organizations require internal control system technological applications in fraud prevention as well as enhance weakness areas in the business to be available at any part of the service or product availability the day or night. These organizations have realized that with centralized and distributed computing and highly available fraud prevention components, their technological presence protects the bank, employees, and customers can be greatly benefited. Today, many organizations largely depend on the manipulation of business using technological applications to achieve their strategic objectives. Accordingly, CBE invested huge capital and tried to implement NG|Screener fraud prevention project for monitoring and controlling bank system activity, identifying weaknesses/loopholes of business systems, and analyzing the behaviors of workers in the banking areas. The purpose of this study is to evaluate the role of NG|Screener project on fraud prevention in the commercial bank of Ethiopia. A descriptive research approach was selected for this study. Data were collected for the study questionnaires and documentation. The collected data were analyzed and interpreted using the descriptive analysis technique. The main role of the system is to mitigate and reduce the challenges of fraud in core application areas, investigate fraud activity across the banking application systems, improve internal control frameworks, and positive impact on the internal control system components (control environment, monitor activities, control activities, information and communication and, risk assessment) using the system big data analysis and sniffing data 24/7. The research findings will give insight to those banking organizations in Ethiopia that plan to implement by understanding the role of this project properly. This research helps to identify the major roles in the implementation of the NG|Screener projects.

Key words: Fraud, Internal Control, NG|Screener, Investigation, Fraud Prevention

CHAPTER ONE: INTRODUCTION

1.1. Background of the Study

In today‘s competitive global business environment change and complexity are common and incorporated into the day-to-day business activity. When working in an environment of constant change and increasing complexity, companies should be competitive, productive, and profitable to stay in the business. On the other side in the competitive and complex environment fraud risks are challenged in technological, management control, policies, and procedures issues/gaps. According to (Markowski & Mannan, 2008) explained Internal Controls system is a critical component of bank management and a foundation for the safe and sound operation of banking organizations. A strong internal control system can help to ensure that the goals and objectives, as well as the visions of a Commercial Bank of Ethiopia, will be met, that the bank can accomplish long-term profitableness targets, and maintain reliable monetary and social control reportage. Such a system or technologies can also help to ensure that CBE will comply with laws and regulations as well as policies, plans, internal rules, and procedures, and decrease the fraud of unexpected losses or damage to the bank‘s reputation and achieving the vision and mission as well as customer satisfaction by protecting from any fraud risk. A system of Internal Controls potentially prevents errors and fraud through monitoring and enhancing organizational and financial recording processes as well as ensuring compliance with pertinent laws and regulations (Rae & Subramanian, 2008).

The banking industry is one of the highly affected industries and it requires implementing different mechanisms and adopting various projects to prevent and mitigate internal fraud risks starting from the front end (business activities) to the backend (IT administrators) for monitoring and controlling. (Beirstaker et al., 2005) proposed several fraud prevention techniques. These a range of strategies consist of fraud policies, cellphone hotlines, worker reference checks, fraud vulnerability reviews, seller contract critiques and sanctions, analytical critiques (financial ratio analysis), password protection, firewalls, digital evaluation, and other forms of software technology, and discovery sampling.

Fraud is a discussion that receives a high level of consideration from regulators, auditors, and the public due to increasing corporate failures, and abuse of corporate image. Most fraud cases happen within organizations rather than in external dealings. Contrary to common belief, 68% of fraud

cases occur within organizations by employers and employees, with the rest externally by those in the value chain (KPMG, 2014). The Association of Certified Fraud Examiners (ACFE)'s 2014 Report to the Nations on Occupational Fraud and Abuse suggests that companies lose up to 5% of their revenue annually to fraud.

The banking industry can be considered as factors, strategies, and organizations that lead to effective financial markets and access to capital and financial services (World Economic Forum, 2012). The contribution of banking sector improvement to monetary growth is vital equipment due to the fact they promote economic growth, develop private sectors, make bigger liquidity to mobilize neighborhood savings, enhance bank competition and improve a larger range of financial institutions (Paul, 2004). Fraud is a major difficulty to the whole banking industry; no bank is immune to it and on all sides of existence (Olorunsegun, 2010). The banking public expects accountability, fairness, and transparency in their daily operation for effective intermediation through effective internal controls. This implies that internal control systems play a positive role in the growth, productivity, and sustainability of monetary institutions (Njagi, 2009; Kiprop, 2010).

Fraud impacts in commercial bank of Ethiopia in several areas including financial, operational, and administration areas of core systems. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. The losses to reputation, goodwill and customer relations can be devastating. Fraud in general, inflicts untold hardship on banks and customers, as most bank failures are associated with large-scale frauds. Therefore to handle all challenges and improved the banking internal control environment effectively, and efficiently and struggle with the negative impact of fraud, the bank implemented different technological systems. So this research intended to evaluate the role of NG|Screener project implementation in Fraud Prevention in the occurrence of fraud risk in the banks.

1.2. Statement of the problem

The banking industry is now growing fast and gaining more and more positions in the country economy of Ethiopia. However, by establishing more banking services, the chances and rate of fraud occurring in the banking industry would also increase. (Chelangat, 2014) stated that Fraud is a universal problem and influences every business, industry, and organization. It leads to losses that continue to cause a significant problem for industries, even though significant progress in fraud prevention and detection technologies. Frauds carried out by bank employees are an

enormous global problem. In its 2022 Report to the Nations, the Association of Certified Fraud Examiners (ACFE) assessed 2,110 cases of internal fraud from 133 countries, which led to estimated losses of more than $3.6bn. Banking and Financial Services accounted for the largest share of internal fraud cases examined by the ACFE, with 15.4% of the total. Commercial bank of Ethiopia has the vision to be a world-class bank by the year 2025 and the bank implements many IT projects including fraud prevention technology. Therefore, due to the rapid growth of banking industry innovation and technological growth in Ethiopia and the shortage of studies conducted in evaluating fraud risk systems in commercial bank of Ethiopia, it is important to attract the attention of researchers to investigate and evaluate the role of internal control system projects on fraud risk prevention in CBE to prevent fraud at the early stage as this type of businesses might provide major income for the country in future. Fraud prevention in the internal control system is not easy to be implemented especially when it comes to complex businesses which have a complex environment and require high costs. According to COSO (1994), the difficulty of cost-benefit willpowers is compounded by way of the interrelationship of controls with commercial enterprise operations; where control is integrated with, or build into, management systems and business processes and procedures, it is difficult to isolate either their cost or benefits form the institution. This shows that, by applying the internal fraud prevention systems, CBE will bind with the company's business processes and costs incurred in that case normally won't be too costly and the advantages of having an effective internal control system are always more than the expected. Lack of Internal fraud risk controlling system in the banking industry and application systems loopholes with weak internal control in the business might give the internal environment a golden opportunity to be involved in fraudulent activities that may cause serious and harmful to the organization. Fraudsters exploit and explain how advanced anti-fraud technologies can struggle with it. Bank employees are distinctively well placed to discover and take advantage of weaknesses in their organization's internal controls – perhaps by abusing their level of access to the bank's IT systems or by targeting dormant accounts.

This research reflects internal control systems have a very important role in the prevention and mitigation of fraud and cannot be undermined especially by the commercial bank of Ethiopia. The lack of an effective internal control system is the major cause of bank fraud. Managing, controlling, and monitoring a widespread internal control system, is robust and sufficient to stand against the tricks of fraud. Most of the research display that the achievement of the internal management

system relies upon on wonderful internal control subculture to promote continuity of operations and to ensure liquidity, and the solvency internal control system plays an undeniable role. However, fraudulent practices are growing and up to date so to manipulate this state of affairs Banks need to have in the area a complete internal control administration technique to identify; measure, monitor, and control internal systems as well as fraud prevention effectiveness.

Therefore this study examines the above-mentioned gaps by clearly evaluating internal fraud risk prevention/mitigation by the role of the internal control system. Hence, the purpose of this study is to evaluate the gaps in CBE made on the causes of internal fraud/risk and the effectiveness of internal control systems of commercial banks of Ethiopia. This is the gap that this study wants to fill. The aim of this study is therefore to evaluate the role of NG|Screener project in fraud prevention of core application and server systems environments in commercial bank of Ethiopia for their fraud management performance.

1.3. Research Questions

- What are the role of NG|Screener project implementation on internal Fraud Prevention challenges of Commercial Bank of Ethiopia?
- Does NG|Screener project implementation effective in internal control system components preventing and mitigating of the occurrence of fraud in commercial bank of Ethiopia core systems?

1.4. Objective of the Research

1.4.1. General Objective of the Study:

The general objective of this proposal will to evaluate the role of NG|Screener project on Fraud Prevention in the cause of Commercial Bank of Ethiopia.

1.4.2. Specific Objectives

Fraud in Commercial Bank of Ethiopia is comparatively high and this has disturbed the growth and development of the organization. The specific objectives of the study are that:

- ✓ To assess the role of systems fraud prevention in different frauds challenges on core banking systems across the banking environment.
- ✓ To evaluate the relevance of system role on internal control system improvement and enhancement for the strength of fraud prevention in the bank.

- ✓ To assess the effectiveness of NG|Screener system role through internal control systems in fraud prevention and mitigation in commercial banks of Ethiopia.
- ✓ To evaluate the role of the project in investigation fraud and risk activity controls in time and quality.

1.5. Significance of the Study

Addressing and emphasizing the role of NG|Screener projects in internal fraud prevention in CBE can be used as the departure point for preventing fraud, improving reliability and availability, and used as a post-knowledge resource for challenges fraud risk trials faced in the banking industry. The study is intended to aid in preventing internal fraud on core systems and environments in commercial bank of Ethiopia employee is at risk if unprotected before the bank implements the system. The study would also aid all financial institutions and other organizations that may have the need assistance systems in the inspection of fraud. Since fraud/risk and some other malpractices are not limited to the banking industry alone. It is hoped that the recommendation and suggestions made in the study would help in the growth and development of banking industries as well as business organization. This research will provide a better understanding of the role of NG|Screener project implementation on internal fraud prevention in commercial bank of Ethiopia internal control areas and financial industries for the company will help to reduce the chance of fraud happen and reduce and protect the credibility of the company.

This research would add more knowledge to the existing literature on the roles of the internal control system in fraud prevention among Ethiopian banking industries.

Finally, the study would be of immense help to all those who wish to carry out further studies on fraud prevention in the commercial bank of Ethiopia or in any other related field.

1.6. Scope of the Study

This study was conceptually focused mainly on the evaluation of the role of NG|Screener project implementation role on in internal fraud risk prevention survey in commercial bank of Ethiopia. This study gives more emphasis for components of internal control system such as control environment, risk assessment, control activity, information and communication and monitoring

areas in core applications and server systems. Commercial bank of Ethiopia is a large organization and provide broad areas of functionality. The study focuses on assess the role of the internal control system in internal fraud prevention exercised on core systems and environments in CBE for a healthy organization perspective. The study will be undertaken in the commercial bank of Ethiopia Head office internal audits, Branch transaction control and Information systems.

1.7. Limitation of the Study

A limitation of a research study identifies potential gaps or problems in the research.

The major limitation of the paper is that it was only based on primary and secondary data in the form of questionnaire and documentation with descriptive type of analysis due to short project work period of time. The constraint of time is the main reason not to use scientific calculations and analytical methodologies.

The secondary data was collected from documents. Due to the sensitive nature of the topic most internal employees are generally not disposed to help, there are other factors beside the challenging all other factors were not be considered in this research because of limited time and other constraints in this advanced technology area that would complicate the study. And some other problems were here and there such as it was difficult to get the respondents in their work place.

1.8. Organization of the Study

The research paper includes five chapters. Chapter one presents the introductory section which embraces background of the study, statement of the problem, objective of the study, research questions, significance of the study, scope of the study ,limitation of the study. The second chapter deals with review of related literature. The third chapter is dedicated to methodology. Chapter four deal with data presentation and data analysis. The last chapter five presents finding of the study, summary, conclusion and recommendations.

CHAPTER TWO: REVIEW OF RELATED LITERATURE

2.1. Theoretical review

2.2.1. Definition of fraud

According to the world globalization and technological transformation, fraud risk patterns frequently change through time, the concept of fraud risk has received attention and different definitions from different scholars, researchers and authors. What is very peculiar to the definitions are interpreting differently in different context. However, the general concept of the term is similar understanding of the logical concepts.

A well-known definition of fraud in literature became given with the aid of the association of certified Fraud Examiners (2016) "as the usage of deception to make a private advantage for one's self dishonestly and create a loss for every other." this will arise and might include sports along with robbery, corruption, conspiracy, embezzlement, property misappropriation, cash laundering, bribery, and a function of believe or fiduciary relationship. (Xu, Zhang et al., 2017) described fraud as any act in which people or a group of people had been made to advantage an undue benefit in a company. The fraudulent act may be committed both by using internal and outside people within the institute with the aid of usually preparing fake financial statement to make people invest within the entity. Fraud is an act made to cheat on human beings and to reduce their self-assurance in monetary institutions (Lang & Wambach, 2013).Such dishonors usually take the form of acquisition finances, material, and even conceal payments in an organization (Klement Neeman et al., 2018). Risk has been described in a range of ways, which are nearly in no way completely real or false, however are beneficial equipment for abstraction and developing frequent focal points (Rosa, 1998; Habegger, 2008). A dictionary definition considers that threat is 'the risk of injury, harm or loss' (Webster, 1983; Habegger, 2008). A dictionary definition considers that risk is 'the chance of injury, damage or loss' (Webster, 1983; Habegger, 2008). The definition of internal fraud is wide. It's far understood to arise while a contemporary or former worker steals, alters or destroys commercial enterprise records (such as consumer facts) or property (including laptop software program or bodily property) for non-public gain. It can contain corrupt preparations concerning extortion from or collusion with others individuals, or can involve falsification of banking economic or different financial institutions.

2.2.2. What is Fraud Prevention?

Fraudulent activities will include a wide vary of cases, as well as concealing, cyber security threats, evasion, fallacious insurance claims, solid bank checks, fraud, and terrorist finance, and is prevailing throughout the banks, government, healthcare, public sector, and insurance sectors. To combat this growing list of opportunities for fallacious transactions, organizations area unit implementing modern fraud prevention and bar technologies and risk management methods, that mix massive knowledge sources with time period observation, and apply accommodative and prognosticative analytics techniques, like Machine Learning, to make a risk of fraud score supported risk matrix. Investigating fraud with knowledge analytics, fraud prevention software system and tools, and a fraud detection and prevention program permits money establishments to predict typical fraud techniques, mention knowledge through automation, manually and regularly monitor transactions and crimes in real time, and decipher new and complex schemes. The four most vital steps within the fraud prevention method include:

• Capture and unify all manner of data types from every channel and incorporate them into the analytical techniques.

• Continually monitor all transactions and use behavioral analytics to facilitate time period choices.

• Incorporate analytics culture into each aspect of the enterprise through data visualization.

• Employ layered security techniques.

2.2.3. Need of Internal Control system projects

According to (Tayntor, 2010), project is described as a unique, finite set of multiple activities intended to accomplish a specific goal and can be differentiated from other activity by its uniqueness. Referring PMBOK Guide (2013), it justifies uniqueness of a project," even though repetitive elements may be present in some project deliverables and activities, this repetition does not change the fundamental, unique characteristics of the project work". The same writer defined it that the nature of project is finite and time-bounded.

There are many researches, which emphasize the necessity and significance of internal control system in the banking system. An inadequate internal control system frequently motives an incapability to detect and stop fraudulent things to do and minimize in the overall performance of the financial institution (Adeyemi et al., 2011). The Basel Committee, (Basel, 1998) alongside with banking supervisors for the duration of the world, has centered more and more on the

significance of sound inner controls. Internal manipulate is a technique affected by using the board of directors, senior administration and all tiers of employees. It is now not fully a method or coverage that is carried out at a sure factor in time, however alternatively it is constantly running at all stages inside the bank. The board of administrators and senior administration are accountable for setting up the fantastic tradition to facilitate a good internal control method and for monitoring its effectiveness on an ongoing basis; however, every character inside an organization need to take part in the process. Internal manage structures are of key significance for firms' interior decision-making strategies and exterior economic reporting quality. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework describes internal control as "a process, effected with the assistance of an entity's board of directors, administration and different personnel, designed to furnish practical assurance concerning the fulfillment of targets concerning to operations, reporting and compliance" (COSO, 2013). Phrased differently, internal controls are mechanisms put in location to grant life like assurance that the banks is well-managed, transparent, and complies with all relevant legal guidelines and regulations. Internal controls truly have an effect on all components of the organization, however the duty for inner controls structures lies in particular with the pinnacle of the company (Li, Sun, & Ettredge, 2010).

2.2.4. The concept of NG|Screener and Theories

NG|Screener is a comprehensive operational fraud risk mitigation solution for Banks. It facilitates internal control by monitoring and analyzing transaction and user behaviors. Using smart behavioral analysis methods, it quickly identifies a typical activity, effectively controls data leaks, and alerts you to potential internal fraud. It offers cross-channel and cross-product intelligent behavioral analysis to ensure fraud risk control, providing real answers to auditors, internal control, IT risk and compliance. It is no exaggeration to say that the biggest fraud hazard that banks face walks via their doorways each and every morning and sits down to work

Fraudsters exploit, and explains how advanced antifraud technologies can combat it. Bank employees are uniquely nicely positioned to find out and take gain of weaknesses in their organization's internal controls possibly by way of abusing their stage of get right of entry to the bank's IT systems or by targeting dormant accounts. But NG|Screener fraud solutions are improving all the time their ability to identify, detect, mitigate and report suspicious activity in real time is becoming the first line of defense against the biggest fraud risk in commercial bank of Ethiopia banking. The framework of NG|Screener system is closely related to the basics Theory

of Fraud Triangle and system theory to compact fraud in prevention and mitigation of fraudulent activities.

2.2.5. Basic NG|Screener Modules

The advancement in information technology (IT) infrastructure is needs for monitoring and controlling of each every activity in every aspect of the bank as well as the technology itself. For the support of technology like NG|Screener system implementation in banking business making the operation controllable and measurable in addition to fraud prevention and mitigation. It is assumed the companies implementing NG|Screener fraud solutions may have multiple scenario of internal controlling system operation and enhance internal control system areas. Hence on line data transfer is done across locations where enabling technologies are used such as Workgroup, Workflow, Groupware, Electronic Data Interchange (EDI), Internet, Intranet and Data warehousing, to facilitate transactions. This is to underline that NG|Screener system is made up of many software components selected based on both fraud and risk prevention/mitigation technical feasibility analysis for given data analyzing units.

- ✓ Dashboard is one of NG|Screener module provides summarized all violation or violation indicator (fraud or risk indicator which lead to fraud) for specific period of time. It consolidate result of fraud risk violation control indicator to have a quick view critical information as a fraud and risk indicators which will be prevention terminology by control activities, analyses risks assessments based, control system server and business environments the metrics.
- ✓ Forensic NG|Screener module is designed to meet legal investigation requirements to pinpoint those events that will lead you straight to the source of an incident and sort out only the key information for proof in litigation cases. It gives the possibility to investigate and analyze from big data visualization in depth from the collected activities and events to control and assess risks in the bank which may IT or business operational data in the big data analysis.
- ✓ NG|Case-Manager It is a workflow engine to manage cases/ compliance issues and define workflows for compliance incident management. It allows user to manage violation and risk indicator activities incidents generated by NG|Screener. It Document incidents and risk/hazard in the huge data analysis and configure workflow for incident escalation,

documentation and validation. This enable the bank to enhance internal audit, risk, compliance as well as policy and procedure review in the bank environment.

- ✓ Control Reporting facilitates NG|Screener fraud prevention risk parameter reports in the communication channel to the specified risk area process by identifying the user and geographical behavioral activity by setting the fraud risk matrix for measurement and corrective action in the respective organs.
- ✓ Console tracking system (CTS) NG|Screener module supports the internal control system by gathers, record and track IT activity data logs from various back server environments, big data analysis and generate reports such as unauthorized activities and fraudulent, super user command activities in every time activity performed and used for investigation purpose.

2.2.6. The Theory of Fraud Triangle

According to (Donald Cressey, 1973 and Olongo, 2013) fraud is probably going to occur due to a mixture of three causes i.e. Pressure, Opportunity and rationalization. Olongo further stated that trusted persons become violators once they imagine themselves as having an economic problem when they are conscious of this problem they are often secretly resolved by violation of the position of monetary trust, and are prepared to apply to their own behavior which allow them to regulate their idea of themselves as trusted persons with their conceptions of themselves as users of the entrusted money. The purpose of NG|Screener project is to handle and mitigate which is challenged in fraud triangle areas in the banking sector core manipulation and operational areas.

2.2.6.1. Rationalization

The attitude of an individual about to commit an unethical act is one of rationalization. The individual/groups manages to justify what he or she is about to do. Some might also suppose they are simply borrowing the stolen goods, or that they want the cash greater than the “big” business enterprise they are stealing from. The individual/groups carrying out the scam frequently justifies the scam. Justifications may comprise, “I will remunerate the cash back”, “They will not miss the moneys”, or “They do not pay me sufficient.” (Hooper and Pornelli, 2010) posits that fraudsters have a specific mind-set that allow them to rationalize their behavior.

2.2.6.2. Opportunity

A chance to commit the act must be present. In the case of fraud, normally a brief scenario arises the place there is a risk to commit the act barring an excessive chance of being caught. In the case of fraud, generally a brief situation arises wherein there may be a chance to commit the act without a high danger of being caught. Most individuals require some form of pressure to devote a crook act. (Wilson, 2004) defines opportunity being the capability to supersede given scam controls. Opportunity is the power and ability of a worker to establish week institutional systems of control and capitalize on committing fraud (Rae and Subramanian, 2008).

2.2.6.3. Pressure

The pressure does not need to necessarily make sense to outside observers, but it does need to be present. Pressures can include money problems, gambling debts, and alcohol or drug addiction. (Albrecht et al., 2006) posits that about 95% of all fraud cases are related to perpetrator's financial pressure. Pressure therefore is an important factor in perpetration of fraud (Lister, 2007). He further determined three types of pressure which include stress due to employment, personal and pressure from external environment. (Vona, 2008).

2.2.7. Systems Theory

A system is considered to be a set of interrelating or codependent constituent parts making a complex or intricate entire intended to achieve a set goal. An organization is a multifaceted system divided into numerous departments which needs a system of control over those subdivisions for its efficiency as well as survival. (Harvey and Brown, 1998) assert that an operational internal control structure needs to be an incorporated system with interconnected constituents as well as supporting values. They further identified controlled situation, accounting classification besides control actions forming key components of internal controls. An internal control structure accessible for a company consist of ; administration oversight as well as control philosophy, control activities, hazard assessment and recognition, information and communication, monitoring actions and adjusting insufficiencies (Grievess,2000). This paper adopted COSOs 1992 integrated internal control structure for internal controls systems with the role of NG|Screener system. The committee of sponsoring organization (COCO) was custom-built in 1980s by the State Commission of Falsified Monetary Reporting (The Treadway Commission) to recognize as well as evaluate the aspects that instigated deceitful company monetary reports as well as make

commendations and has since established to become a thought frontrunner in business risk administration (ERM), internal control, and deception discouragement (Amudo & Inanga, 2009).

2.2.7.1. Control Environment

The control environment helps to set the organization's tone, affecting the control Realization of its persons or employees. It is the basis for all other elements of interior control, offering discipline as well as structure. Control atmosphere aspects comprise of reliability, moral standards as well as ability of the entity's individuals; administration's viewpoint and working style; the way organization allocates power as well as duty, arranges and progresses its persons; and the attention as well as direction offered by the board of managements (COSO, 2011).

2.2.7.2. Risk Assessment

Risk assessment is considered to be the identification as well as examination of applicable hazards which can damage the accomplishment of purposes, creating a base for determining how the hazards must be managed. Fraud as an inherent risk needs to be assessed and anti-fraud programs generated as key to an effective internal control culture. Risks are evaluated to determine the probability of an occasion happening, the effect, as well as hazard patience (IIA, 1999). To determine if hazard administration are operational, pertinent hazard information must be taken and conversed in efficiently across the organization, permitting management to do their tasks. (IIA, 1999).

2.2.7.3. Control Activities

Control activities are considered to be the procedures as well as actions that help to ensure that administration directives are done. They ensure that needed activities are taken to deal with hazards that hinder accomplishment of the entity's aims (COSO, 2011). Control actions, if automatic or manual, have numerous aims as well as functional at numerous administrative and practical levels. Usually control actions that may be pertinent to an examination may be characterized as plans and processes that relate to performance evaluation, information handling, physical control and separation of obligations.

2.2.7.4. Information and Communication

Information as well as communication is considered to be necessary to implementation of control. Information about an administration's idea, control atmosphere, peril control actions as well as performance should be conversed up, down, and across an organization. Relevant information should be recognized, seized and communicated in the time frame that enables persons to do their

tasks. Information classifications offer reports comprising working, monetary as well as compliance associated information that makes it likely to run and control industry.

2.2.7.5. Monitoring

This is the valuation of internal control actions overtime. It is achieved by continuing monitoring actions as well as by distinct assessment of internal control, self- valuation, peer evaluation and internal inspection. There is linkage as well as cooperation among elements creating an incorporated structure that responds enthusiastically to the varying circumstances. The internal control structure is entangled with entity functioning activities for essential occupational motives. Internal control is considered to be the most operational when controls are created into object's infrastructure and they are part of the principle of the initiative 'constructed in''. Control support superiority and authorization initiatives; evade superfluous expenses and allows fast reaction to varying circumstances. Monitoring evaluates the quality of the company internal control actions by tracing and checking the internal control setting and functioning grade and take the essential activities to make sure that internal control function efficiently.

2.2.8. Role of internal control and NG|Screener Project

The studies of p.C and the ACFE stated before screen a few data concerning the prevention and mitigation of internal fraud. The number one prevention tool is tip-offs and finding by accident. This kind of instrument is not easily influenced by corporate governance, because it is linked with company culture, and not with controls. The second best prevention tool seems to be internal control system for fraud mitigating. Internal control is currently the most prevailing mean businesses use to mitigate fraud. The Committee of Sponsoring Organizations of the Tread way Commission was formed to commission the Tread way Commission to perform its task (study the causes of fraudulent reporting and make recommendations to reduce its incidence). COSO established an internal control framework, issued in 1992 and entitled Internal Control Integrated Framework. According to the COSO framework, internal control is defined as:

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

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

If we look at the meaning, it is clear why internal control system is significant as a defense against fraud. The achievement of the first category is to encounter transaction fraud, the second to encounter statement fraud and the third category accomplishment is to protect the organization against fraud for the company. Therefore, internal control can both prevent and detect fraud. We can conclude that internal control is a means to protect an organization against internal fraud, but given the rising occurrence of fraud it is still not adequate as a standalone tool. These studies also emphasize the added value of NG|Screener project implementation well-functioning internal control systems. The internal control framework of COSO is the biggest existing framework on this topic. Some businesses organizations have taken this framework and customized it to their specific needs, for instance the banking industry. In this atmosphere, Basel II is created, with its own inner control section. The goal of this paper to address all roles of NG|Screener in CBE internal control contexts in commercial bank of Ethiopia to control and monitor activities, mitigate the cause and investigation of issues to create a productive banking environment. By addressing the situations of COSO, the general banking system practice in terms of internal control improvement and strength prevention are covered.

2.2.9. Types of Internal Controls

2.2.9.1. Preventive Controls

These are controls that expect potential problems before they occur and make modifications. Additionally they prevent an error, omission or malicious act from happening. A lack of effective prevention techniques spurs much of the research on financial fraud prevention-detection NG|Screener provides back screening of the operational activities of preventive controls consists of: using well-designed files to prevent mistakes, setting up suitable approaches for activities and inform the authorized controller employees activity execution and attempts of wrong doing. (Ahmed, Mahmood & Islam, 2015) noted a scarcity of real-world data related to effective prevention techniques of fraudulent behavior, while (Throckmorton et al., 2015) identified the need to define factors for the development of effective discovery tools.

2.2.9.2. Detective Controls

According to the Office of Internal Audit and Institutional Risk Management (2012), these are designed to discover errors or irregularities when they have passed off. Examples of detective controls are: (1) reviews of performance: management compares facts approximately modern-day

performance to budgets, forecasts, previous durations, or different benchmarks to degree the extent to which desires and goals are being completed and to pick out sudden effects or uncommon conditions that require comply with-up. (2) Reconciliations: A worker relates exceptional units of records to each other, identifies and investigates variations and takes corrective action while essential.

Research by a number of different group's exhibits that internal fraud is detected in a wide sort of methods. Each the association of certified Fraud Examiners (ACFE) and KPMG, in its report global Profiles of the Fraudster 2016, locate that the maximum not unusual approach of detection is casual tip-offs from different team of workers or customers, even though a large percentage of inner frauds come to light through whistle-blowing hotlines. Control evaluations and inner audits are also among the important strategies of prevention, with 65 percent located via inner audit in 2016 and 34 percent through control overview, consistent with the ACFE. However, KPMG's study reported that the equal percentage of inner frauds (14 percent) have been uncovered by coincidence as through internal audits. "Unintentional detection is a sobering reminder that the controls are useless," it says. The UK anti-fraud employer Cifas says that 47 percent of the 409 internal frauds logged through its 172 member businesses in 2016 have been detected through internal controls and audit. It comments: "that is reassuring because it method that the investments made through agencies in these procedures and, in a few times, software answers are offering price. It's also probable that these structures are at least in part answerable for the decrease degrees of recorded internal fraud.

2.2.9.3. Corrective controls

Current studies primarily focus on reactive measures and consequences of financial statement fraud in the bank. A qualitative, multiple-case study inquiry offers the opportunity to examine current practices for detecting and preventing fraud from a participant perspective. The need of Implementation and development of effective fraud prevention tools in the opportunity to remedial internal controls systems. NG|Screener is on of controlling tools help to minimize the impact of a threat, identify the cause of a problem, identify loopholes of the system lead to fraud and correct errors arising from the problem. Additionally they correct problems discovered via detective controls and modify the processing tool(s) and applications to minimize future occurrence of the trouble.

2.2.10. Role of NG|Screener on fraud prevention in CBE.

NG|Screener is a tool used in the fraud prevention in the banking industry to combatting of fraud risk mitigation and enhancing internal controls systems. (Bhasin, 2015b) remarked, "Technology/tools is sort of an ambiguous weapon. On the one hand, perpetrators area unit the employment of it to additionally dishonest schemes; on the various hand, we tend to area unit creating a number of our exceptional development the usage of the identical technology. Beyond question, technological ability will show helpful in fraud finding and interference in banks. As technological ability turns into bigger advanced, dishonest schemes can end up to be bigger complicated, while further progressive fraud choices are developed to fight hackers' glorious efforts." however sadly, the fraud takes on many sorts to be proscribed with any 'single' software package or approach. The cat and mouse sport can continue. Because the panorama of fraud continues to shift, enterprise leaders have to be compelled to be responsive to developments and predictions that may change them to place in effect internal/external controls and structures to help decrease the threat of fraud and preserve them from turning into the other datum (Mueller, 2015). Rather than hoping on reactive measures like whistleblowing, banks will and have to be compelled to take a further active strategy to fraud prevention-detection. A fraud detection and interference software package got to contain a range of approaches—from point-in-time to habitual and ultimately, unendingly for these areas the place the prospect of fraud warrants. Supported key risk indicators, point-in-time (or advert hock) testing can assist discover transactions and activities to be investigated. If that looking for displays symptoms of fraud, normal attempting out or non-stop analysis should be thought of. By investment the strength of knowledge analysis software package, banks will sight fraud faster and minimize the negative impact of large losses as a result of fraud risk.

2.2.10.1. Prevent internal fraud challenge in CBE Core applications.

The following are the foremost important and common kinds of fraud emphasized in Commercial Bank of Ethiopia Bank core technological systems in Administration of fraud prevention series;

2.2.10.1.1. Unauthorized Withdrawals

As (Olongo, 2013) cited in his study that Unauthorized Withdrawal involves the withdrawal or transfer of money from individual's bank account without proper authorization or permission by the owner. Such frauds are the results of a person intentionally, or unintentionally, revealing their private information like personal identification numbers and password to criminals or other

persons. Forgeries of customer's signature to withdraw illegally from individual's bank account or forgeries of other money from one account to another or withdrawal of money from one account to a different through the utilization of ATM (Automatic Teller Machine) according to Ebe (2006, as cited in Olongo,2013). The counterfeit could also targeted on "saving accounts, deposit accounts, current accounts and transfer instruments" (Olongo, 2013, p.18).

2.2.10.1.2. Unauthorized Use of Credit or Debit Card

Unauthorized Use of Credit or Debit Card is a transaction involving the charging of expenses or purchase of products and services without the permission of the card owner. Such transactions may occur as a result of credit or debit cards that are lost, stolen, not received, issued on a fraudulent request, fake or other fraudulent situations (Olongo, 2013).

2.2.10.1.3. Illegal Foreign Exchange Trading Scheme

(Olongo, 2013) explained that illegal Foreign exchange is buying or selling of foreign currency by person or institution who is not legal dealer. Buying or selling of foreign currency by a resident who is not certified dealer, with a person outside the country, or by a dweller who has not obtained the authorization of the regulator of Foreign Exchange.

2.2.10.1.4. Illegal Deposit Taking

Illegal Deposit Taking is an act of receiving, taking or accepting of moneys, precious metals, precious stones, etc. from members of the community that guarantees a repayment with interest or returns in money or money's value without a legal license from the concerned bodies under the financial Banking industry Act 1989 (BAFIA, as cited in Olongo,2013).

2.2.10.1.5. Fraudulent Money Transfer

(Akinyomi, 2012, as cited in Chelangat, 2014) in his study on the assessment of fraud in the Nigerian banking industry explain fraudulent money transfer as a fraudulent demand or change a legal Funds Transfer Request for the aim of perpetrating fraud. The fraudster will then conspire with Bank employees to withdraw the funds.

2.2.10.1.6. Theft and Embezzlement

Theft and embezzlement is another type of fraud which includes the unlawful collection of financial items like cash and cheque (Akinyomi, 2012, as cited in Chelangat, 2014).

2.2.10.1.7. Abuse of Administrator Privileges

Abuse of administrator privileges is one of the key inner-fraud risks facing economic establishments. It characterizes an inevitable source of difficulty due to the fact some

extraordinarily trusted IT staff will continually require "super user profiles" to function their day-to-day responsibilities or carry out crucial maintenance on the core banking application systems.

2.2.10.1.8. Transaction Reversal and deletion

A hassle in rising markets, where bank internal team of workers reverse deposit, delete deposit transactions after the purchaser has left the department and steal their money.

2.2.10.1.9. Account and customer Manipulation

Where staffs take away charges or adjustment interest rates on loans or credit limits, typically to benefit their family or friends. On the other hand internal staffs amend customer and account data for preparing fraud by changing without customer or controller concern.

2.2.10.1.10. Loan Applications

Another frequent tactic is to steal a customer's private details and use them to practice for loans or credit score playing cards in the customer's name. Hiding Losses

Losses on banking consumer's funding portfolio can be hidden via briefly taking cash from the financial institution's suspense account – used to preserve finances pending reconciliation and allocation to the very last account – and shifting them into the purchaser's portfolio account to boom the balance. After the customer meeting, the funds are moved back to the suspense account.

2.2.10.1.11. Four Eyes Violation

The bank have four eyes principle to make any activity but normally occurs where two or more employees work together to avoid Static controls by approving fraudulent payments in violation of the Four Eyes Rule. The other way of four eyes violations is a risk that the same employee could both create and authorize a fraudulent transaction. However, even where such a control exists, a fraudster can get round it by signing in with another employee's user credentials to validate the rogue transaction.

2.2.10.1.12. Data Theft

Internal bank staffs embezzled Bank customers' data, including pin numbers and account details, customer identity, account balances are vulnerable to theft by members of internal bank staff. This information can then be sold on the black market or they used indirectly for fraudulent activity.

2.2.10.1.13. IT Changes at the Back End

Internal Staff with IT administrator privileges can play a key role in internal frauds by themselves or with collaboration of other IT staffs/ non-IT staff (business) through granting administrator rights just long enough to allow them to approve a fraudulent transaction/activities.

2.2.10.1.14. Application system loopholes

System are not error free by the nature which will be analyzed every time and need improvement by closing the identified gaps and fraud opportunity loopholes for the effective bank operation in the banking operational activity. Concerning the effectiveness of fraud prevention methods. (Rashidah & Irda, 2014) suggest that banks should not depend solely on a single method to cope with fraud. The banks need to alternatively put in force tests and balances to perceive loopholes in the financial institution internal control gadget and to improve the techniques for greater advantageous fraud prevention.

2.2.10.2. Fraud risk Investigation

Fraud risk investigation forensic analysis are safeguarding and retrieval of electronic information for evidence purposes, and electronic discovery for litigation support. Today in banking industry like commercial bank of Ethiopia every transactions are being completed electronically application within the business. Therefore the role of prevention systems in the fraud risk investigation and forensics have great impact on Significant information that may exist, what form and format it retains, where it could be located and accessed, and, most important, how to gain access to it, could be the most significant factor in prevailing in litigation or proving fraud risk case encompasses a bank, in preventing fraud schemes from occurring, investigating fraud schemes that have occurred, and assisting organizations in implementing better controls and procedures in response to a fraud scheme having been committed. NG|Screener plays a role in CBE for fraud happened and investigate of the root cause of the fraud to mitigate and provide solution in a big data set.

2.2.10.3. Internal Controls Policy and procedure enhancement

A robust internal control system policies and procedures are required. These includes financial transaction documentation, procurement processes, product design projects, product testing, risk management, fraud risk, segregation of duties, authorization procedures, adequate documentation, independent checks, physical controls, system management/implementation and internal audits. This is important aspects for banking industry for determine which parts of the company are at a higher fraud risk than others and continues evaluate your control designs including documentation, training, segregation of duties, and feedback loops. Internal controls necessity and appropriately implemented, and staff members, non-staff personnel, suppliers, implementing partners and third parties are informed about fraudulent and other prohibited practices, and their consequences, can curtail the occurrence of such practices. Banks applied combined policy/procedure and

information technology-driven based preventative and mitigation controls systems into internal systems. NG|Screener is one of the preventive detective system for organizing and up-to-date standardized internal control system policy and procedures for the competitive banking sector like commercial bank of Ethiopia.

2.2.10.4. Risk management system

Risk management is described because the 'system of information and dealing with dangers that the entity is necessarily problem to in attempting to gain its corporate objectives (CIMA reliable Terminology, 2005).All internal control procedures must undergo through a risk assessment. Identify which failures are most probable to broken up and distress your organization. Fraud risk assessment is an integral and key component of commercial banks Risk Management. The aim is to help management to identify and evaluate areas of programmatic and operational activities that are most vulnerable to fraudulent and other illegal practices, and priorities where CBE should focus its resources for prevention and mitigation. NG|Screener fraud risk assessment process may be repeated periodically utilizing lessons learned, especially for longer-duration programs and operations, or where material changes are made to the design of the plans and operations during their implementation.

2.2.10.5. Management Control System

Management control is the first line of defense in fraud risk activates in the banking industries. There is heavy reliance on assessment controls that involve trend and predictive analyses, organizations should remember whether or not the predictability of effects remains dependable, given the rapidly converting surroundings. Evaluation controls may require more comprehensive evaluation, or opportunity weighting in preference to factor estimates that allows you to additionally necessitate extra documentation to correctly evidence the overall performance of the assessment. Therefore the management must build strong four eyes principles and employee monitoring systems.

- ⇨ Four Eyes principle is an extended-hooked up banking practice that calls for group of workers to attain validation from a colleague for sure actions, which includes payments above a certain amount. This practice is essential part of the so-called First Line of protection controls that banks installed area to prevent inner fraud, but even if this control is coded into the financial institution's systems it has been shown to be vulnerable to abuse. It's far obviously possible for team of workers to collude and so avoid the four Eyes precept,

however internal fraudsters may also be able to steer clear of this manage via stealing a colleague's machine credentials and signing in under their identity to validate a fraudulent transaction. Team of workers who leave their session open whilst far away from their desk go away the bank susceptible to this kind of assault. Further, financial institution group of workers with realize-ledge of back-office rules can also recognize the transaction size that triggers the requirement for a 2d individual to validate it, and might consequently strive a chain of smaller bills beneath the trigger stage. Modern anti-fraud systems can flag cases of this nature by using employing cumulative price controls that come across more than one small bills under the four Eyes limit. They also can flag times wherein two members of body of workers sign on to the device from the same system in short succession, indicating feasible use of stolen credentials to authorize a transaction

- ⇨ Employee Monitoring systems designed to prevent internal fraud risk depend on monitoring, whether through controls that require staff to have certain actions validated by colleagues, or using technology that notes and records each individual's accomplishments on the bank's IT systems and flags any behavior that is mistrustful or unfamiliar. Monitoring is an essential part of modern anti-fraud systems because historical data on individuals' behavior must be gathered to low the creation of profiles against which future behavior can be compared to detect unusual or suspicious activity. Employee monitoring is permitted through regulation in most jurisdictions, although businesses ought to disclose to their group of workers that monitoring is taking location and they will be required with the aid of law to perform an effect assessment before it may be implemented. Covert tracking is usually authorized simplest in very restrained occasions related to the investigation and detection of crimes. Making staff aware that their use of the banks IT systems will be monitored and controlled is likely to deter many potential cases of inner fraud. Attractiveness of the business enterprise's right to display body of workers and its tracking policies will generally shape a part of the employment contract.

2.2.10.6. Employee system Behavioral Profiling monitoring

NG|Screener delivers the role of internal activity profiling in the bank internal control measures. Behavioral analysis of the bank is robust way of fraud risk prevention/mitigation mechanisms. The system provides for the performance management system of each employees by evaluating day to day activities in the banking system. Fraudsters are known to exhibit certain behavioral traits.

According to ACFE's 2022 Report to the Nations on Occupational Fraud & Abuse (www.acfe.com/rttn), summarizes the most common occupational internal fraud risk metrics to three areas at top level. One is Asset misappropriation, Secondly, financial statement fraud schemes and third category is corruption. Behavioral profiling lies at the coronary heart of technology-based antifraud structures and represents a fundamental latest develop in fraud detection made feasible with the aid of the growing strength of Big Data analytics. Profiling complements rule-based totally controls by studying very large quantities of facts at the historical behavior of every worker and customer to create a profile that describes the typical way wherein they use their account: how, when and in which they get entry to it; who they normally make bills to; the sums commonly involved; and so forth. The machine then compares each motion that takes location on the account in opposition to the profile and rankings it in opposition to a range of danger indicators to estimate the possibility that the transaction is a result of inner or external fraud.

2.2.10.7. Cyber Security System

Companies may face potential increased vulnerability to cyber- assaults due to far flung work environments, such as larger susceptibility to phishing assaults, malware, shoulder sniffing passwords, change credentials, illegal use of other computer system and others. Nowadays, cyber protection has been a daily problem that can be determined everywhere, from the news that reviews spam, scams, frauds, and identification theft, to educational articles that talk about cyber warfare, cyber espionage, and cyber protection (Dunn-Cavelty, 2010). These drastically carry the trouble of cyber protection end up greater necessary and applicable in latest years. Consequently, corporations will want to assume about growing focus and training associated to cyber security, and may also want to beautify their protection monitoring abilities to observe and mitigate fraud danger threats and viable infections, as properly as operate vulnerability assessments and different AI based totally checking out to make certain appropriate cyber safety measures are in area for banking industries/ monetary industries to decrease and decreased organizational fraud danger scenarios. (Dewar, 2014) explains that 'the purpose of cyber protection is to allow operations in our on-line world free from the chance of bodily or digital damage. NG|Screener system enhances internal cyber security by controlling and mapping user, and the domain are client operational environment which each detailed activities and manipulation cyber fraud risk prevention.

2.2.10.8. Enhance Compliance

Compliance threat is described as the threat of criminal or regulatory sanctions, fabric economic loss, or loss to popularity that a Bank may additionally go through as a end result of its failure to comply with laws, regulations, rules, associated self-regulatory standards, excellent enterprise practices, inner insurance policies and tactics and codes of habits relevant to its banking things to do (CBK 2012). (Haynes, 2005) stated, continues compliance feature as the characteristic that ought to facilitate the implementation and preservation of the compliance culture, organize for or furnish compliance framing, suggest on regulatory matters, habits monitoring, keep line of verbal exchange with the regulator, take care of regulatory issues, behavior reviews, grant reviews and training to management, help in identifying, assessing and managing regulatory risk, control internal, exterior and inter-relationships, and flip regulatory burden into aggressive benefit (e.g. such as recommending IT solutions, legislation and guidance.

The 2016 Report to the Nations by way of the Association of Chartered Fraud Examiners (ACFE) states that 40.7 percent of inside frauds are in no way stated to the authorities, usually to keep away from reputational harm to the employer in question. However, in spite of the great reluctance to file inner frauds, financial institution personnel typically face justice in such cases. In 2017, 4 contributors of workforce from a British financial institution have been jailed alongside with three exterior accomplices for a complete of 38 years after passing on the small print of dormant bills retaining giant balances. In July 2017, a financial institution teller in the US used to be charged after stealing $185,000 from a homeless consumer who had introduced in a sack of money to credit score in a present account with the bank. However, in some rising markets, weaknesses in the prosecution device have intended that instances of inner fraud are no longer delivered earlier than the courts or fail due to lack of evidence, leaving perpetrators free to practice for a job at some other bank. Blacklists are regularly used to weed out suspected fraudsters.

2.2.10.9. Internal Audit System

Internal auditing is an independent and third line of defense in banking industry, the objective is assurance and consulting activity designed to add value and improve an organization's operations. Its function consists of detecting, preventing, and monitoring fraud dangers and addressing these dangers in audits and investigations. It ought to think about the place fraud chance is existing inside the enterprise and reply accurately via auditing the controls of that area, evaluating the doable for the incidence of fraud and how the company manages fraud threat (Standard 2120.A2) thru risk

assessment, and audit planning. It is now not inside audit's direct duty to forestall fraud going on inside the business. This is the responsibility of management as the first line of defense. Therefore internal audit is very relevant to ensure the efficient utilization of resources, control misappropriation and combat fraud and misapplication of the resources of a company (Badara & Saidin, 2014). Internal auditing applies concepts in an organization to make certain effectively in the increase and improvement of an agency main to sustainable economic conditions. (Alzeban & Gwilliam, 2014) believe that failure in an organization is the consequence of week implementation of internal audit practices. NG|Screener is one of the important tools in internal audit actions and fraud investigation by analysis of historical and real time operational activities, provide pre audit risk assessment on different geographical area activities.

2.2.10.10. Improve three line of Defense

In banking industry and financial institutions, there must be improve strong and mature organizations fraud risk controlling and monitoring prevention/mitigation line of defense models. Fraud doesn't happen in a vacuum; organizations often enact specific internal controls designed to prevent, detect, or mitigate any attempted wrongdoing. Since the Global Financial Crisis of 2007–09, the design and implementation of internal control structures has attracted serious educational and expert attention. Much lookup on the effectiveness and traits of inner audit features has been performed beneath the sponsorship of the Institute of Internal Auditors Research Foundation (IIARF) and posted in educational and expert journals. The "three strains of defense model" has been used historically to mannequin the interplay between company governance and interior manage systems. We think about the current three-lines-of-defense mannequin may want to be significantly greater through giving it a particular center of attention on the law of banks and insurance plan companies. The suggestions issued with the aid of the Basel Committee e on Banking Supervision (BCBS) in 2015 on company governance ideas for banks emphasize the significance of appropriate hazard administration procedures, including, in particular, "an wonderful impartial hazard administration function, beneath the course of a chief threat officer (CRO), with enough stature, independence, assets and get right of entry to the board." Furthermore, "the sophistication of the bank's risk management and inside manipulate infrastructure must hold tempo with modifications to the bank's danger profile, to the exterior threat panorama and in enterprise practice" so as to identify, screen and manipulate dangers on an ongoing bank-wide and individual-entity basis.

However, the effectiveness of these measures in deterring and uncovering fraud can depend on many factors and can change over time. Consequently, it can be helpful for organizations to benchmark their own anti-fraud controls against those of other organizations.

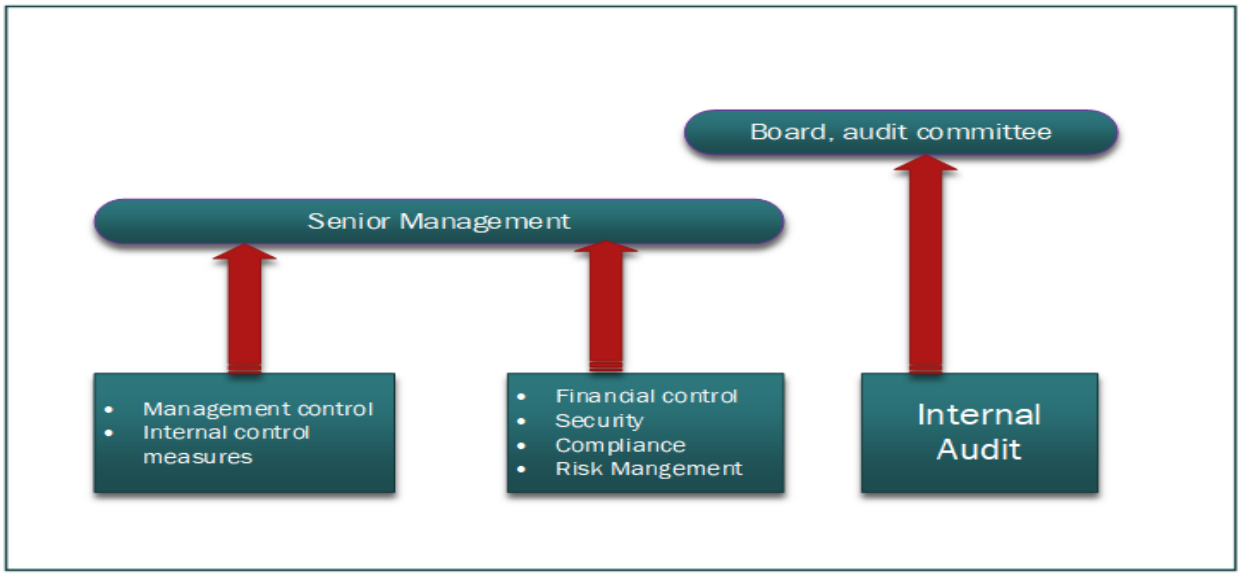

Figure 2.1. The Three Lines of Defense Model (Source IIA (2013))

2.2. Empirical Review

Empirical studies have pointed to the role of four major factors, namely, loopholes in banking system, non-compliance with procedures, ineffective supervision, and control of working of bank's operation of branches/process (Neupane, 2020). As per the study of the world's well-known auditing and tax Consultant Company KPMG (2006), and Deloitte a UK company (2015) the causes of fraud are poor internal control, lack of ethical value, collusion between employees with outsider party, management override control of management and dissatisfaction among employee. (Micheni, 2016) found, internal control is an important component in preventing and supporting successful operation and productivity in any firm.

The study of (Gitau et al., 2016) in Kenya through descriptive studies design additionally observed the position of robust internal manage systems in decreasing fraud. Another factor indented to have a crucial role in banking fraud is the information technology and poor data management. With the advent of internet technology, both opportunities, as well as challenges, emerged in online banking. According to (Aribake, 2015, one of the main difficulties of internet technology is the

issue of security. (Bhasin, 2015) stated that technology is a two-sided sword; on one hand, it has brought much development; on the other hand, perpetrators use it for fraudulent works. (Swain & Pani,. 2016) concluded that cybercrime has become a new menace of the day with the advent of technology. Technology may be abused from inner and outer sides; employees from in-house and fraudsters from outside misuse technology. Computer frauds can also occur due to fallacious enter gadget, application manipulations, transaction manipulations and cyber thefts. Statistics anomaly will be because of untrained personnel or by means of intentional wrong information input. In the words of (Bhasin, 2016), lack of customer and staff awareness can result in the failure of even the best technology solutions. Available studies have also pointed to the role of legal system or projects in bank fraud. Fraudsters dare to fraud in weak regulation and control (ICC business Crime services, 2002).

Incongruous results have been established regarding internal control system instituted and the occurrence of scam (Beasley, 1996; McMullen, 1960; Dechow et al., 1996). Nevertheless, effectiveness of internal controls have reduced fraudulent practices within companies prone to fraud (Abbott et al., 2000).

Researchers posits that incentives, pressure and rationalization forces fraudsters to focus on weaknesses within the internal controls that could permit them to commit fraud (Mars Group, 2008). In Kenya particularly, GFRP issued directions to all accounting officers in all government bodies to ensure an effective internal control units to shield against fraudulent practices. It further directed the accounting staffs to make sure that the system of internal inspecting occurs under the direction as well as regulator of an Internal Accountant General to assess the efficiency of internal controls.

Organizational environment effect on scam has been steadily determined in the past studies. Worker stealing has been discovered to be affected by company's work environment (Weber et al.,2003;Appelbaum et al., 2006; Kulas et al.,2007) as well as staffs attitudes toward morality (Greenberg, 2002).

The significance of internal control tools in cutting fraud-bent behavior, especially worker scam, has been inspected. Where upon management devotes attention towards controls instituted, perpetrators of fraud were likely to reduce Holmes et al 17 (2002). Similar study established that admittance to numerous control mechanisms only does not control losses because of fraud (Holtfreter, 2004). Flouting the Scam Triangle is the main to scam discovery. Breaking the Scam

Triangle suggests that the company should remove one of the essentials in the scam triangle to decrease the possibility of deceitful actions. Out of the three essentials, elimination of opportunity is most explicitly influenced by the structure of internal controls and usually offers the most illegal route to discovery of scam (Cressey Cendrowski, et al, 2002).

The importance of internal control mechanisms in dealing with counter work behavior, specifically employee fraud, has also been investigated in other related studies such as O‟Leary et al. (2006). Employee theft has been linked to similar studies on employee perceptions of the certainty and severity of organizational sanctions (Hollinger and Clark, 2001). Internal offenders and fraud are less likely to occur when top management strongly supports internal control, according to Holmes et al. (2002). Another study indicated that simply having access to multiple control systems does not prevent fraud losses (Holtfreter, 2004).

2.3. Conceptual framework of the study

A conceptual framework is a brief description of a phenomenon that is frequently accompanied with a graphic depicting the study's primary variables. It shows the interaction of variables under study (Mugenda, 2008). The researcher believes that when assessing internal fraud prevention and mitigation on commercial bank of Ethiopia internal control systems must be considered as essential tools for the study. Thus, the researcher selects internal control systems which are control environment, risk assessment, information and communication, control activities, and monitoring activities as independent variables while NG|Screener fraud prevention at commercial bank of Ethiopia as dependent variable.

Based on the review of both theoretical and empirical studies on banks fraud and risk prevention/mitigation of commercial banks of Ethiopia, the following conceptual framework guiding this study was developed. In assessing internal fraud risk prevention and mitigation, the evaluator must understand the operations of the five components, the intent of the principles and assumptions underlying the operations of the control components and how they are applied across the organization. The researchers in assessing internal fraud risk prevention system of commercial banks adopts some of COSO‘s principles and assumptions of assessing internal fraud risk and mitigation.

To summarize theoretical literatures, empirical literatures and system environments discussed and reviewed before, a conceptual framework is developed for this study.

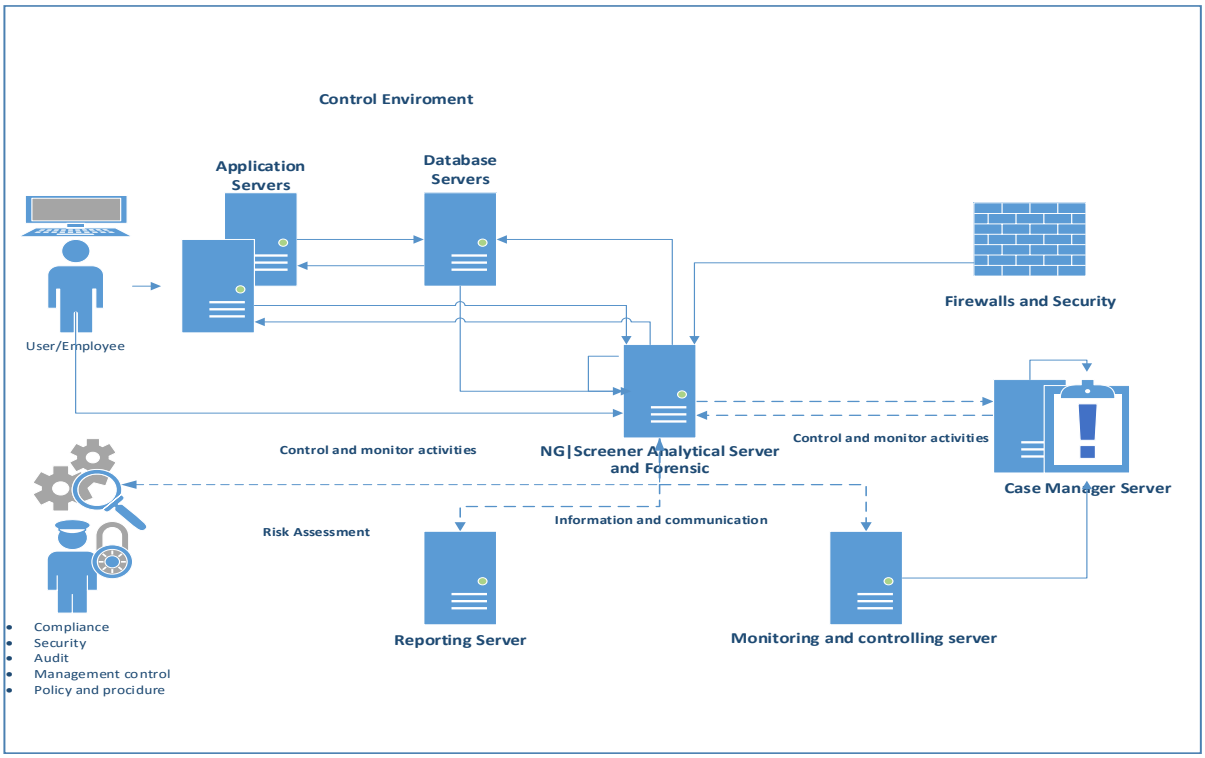

Figure 2.2. Logical conceptual model of NG|Screener on fraud prevention with COSO frameworks

.Based on the theoretical, empirical and above diagram, the conceptual relationship/framework between variables is developed as;

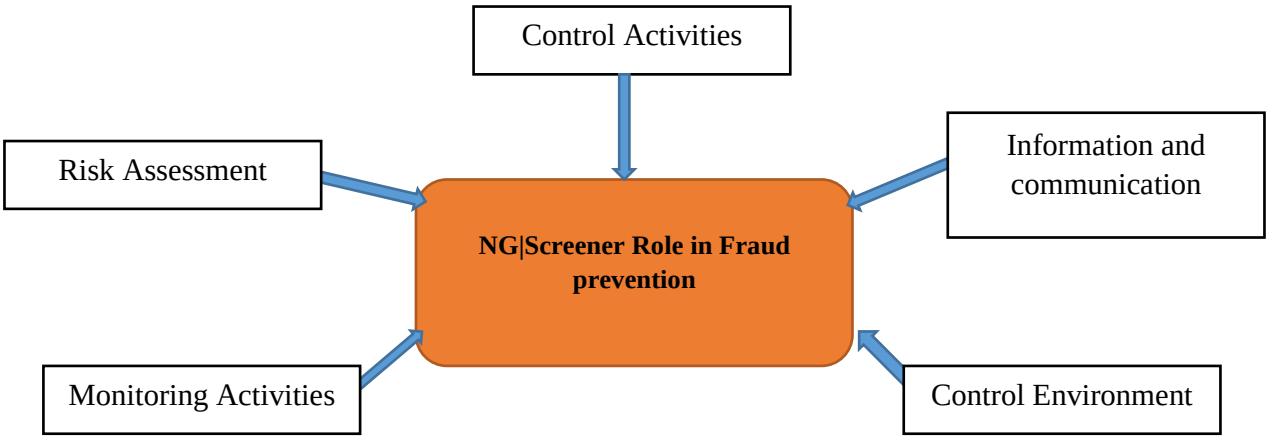

Figure 2.3. Conceptual Framework model (source: COSO's ICF)

CHAPTER THREE: RESEARCH METHODOLOGY

Introduction

This chapter includes sections such as the methodological approaches used in the research design, sampling, and the population. It additionally consists of the instruments used in the research, for gathering the data as well as its legitimacy and trustworthiness.

3.1. Research Design

A cross-sectional survey with a quantitative methodological approach was adopted in the study, to achieve the purpose of examining the role of NG|Screener on internal fraud prevention in the case of commercial bank of Ethiopia. (Schutt, 2011) described a quantitative learn about as a rigorous, goal, and systematic method of acquiring numerical records and the use of manipulated measures and statistical evaluation to get rid of contaminating factors. The quantitative methodology was adopted because, as Quinn (2010) explains, the quantitative approach provides the possibility of measuring the reactions of a great number of people to a limited set of questions. The current study is descriptive because it focuses on describing the level of coverage of banks to the role of NG|Screener in fraud risk prevention and the level of fraud risk prevention technology in the core system areas. Therefore, this study used a descriptive research method due to the limitation of time and adopted only a quantitative approach to gain insight regarding the study area to answer the research questions. Respondents from the bank were sampled from main departments, namely, internal audit, internal control, and IT. The study was therefore a quantitative study on evaluation of the role of NG|Screener project on fraud prevention in the Commercial Bank of Ethiopia.

3.2. Population and Sample Size, and Sampling Techniques

3.2.1. Target Population and sample size

Castillo (2009) defines target population as, referring to the entire group of individuals or objects to which researchers are interested in generalizing the conclusions. The study's population of interest are sampled employees from the bank staffs who were experience and role related in the fraud analysis and risk mitigation areas in the commercial bank of Ethiopia ware considered as the target population. The study targeted the respondents within the internal control and IT area. The targeted participants included sampled employees from internal audit, internal control and IT departments. Overall, sixty (45) employees from the three targeted CBE departments constituted the population of the study.

3.2.2. Sampling Technique

According to (Price, 2009), purposive sampling is a form of non-probability sampling in which decisions concerning the individuals to be included in the sample are taken by the researcher, based upon a range of standards which can also consist of expert information on the research issue, or ability and willingness to take part in the research. Some study designs require researchers to decide which individual participants are most likely to provide useful data, both in terms of relevance and depth. In addition, this method was used when the members of the entire population do not present the same performance.

Purposive sampling was preferred in this study, and participants were project managers, team leaders, functional managers, and team members who have more than three years of experience in the area. Thus, the nominated samples ware assumed to have sufficient knowledge and experience in fraud risk mitigation and prevention. Thus, the sampling technique used for the selection of questionnaire respondents was the purposive sampling technique

3.3. Data Collection methods

3.3.1. Source of data

The main sources of data in this study were the commercial bank of Ethiopia. The primary data sources were selected departments and functional staff. The secondary sources of data ware obtained from documents and proposals. For the descriptive type of research, primary data ware obtained through a semi-structured questionnaire survey and documents. To conduct the study, semi-structured questionnaires were prepared to obtain the required data from selected sample respondents.

3.3.2. Instrumentation for Data Collection

The primary data collection instruments were questionnaires designed. Data collection tools that were used in this study are questionnaires, which were semi-structured and enabled the researcher to collect the data. The questionnaire was created by the researcher based on the study's objectives.

3.4. Data Collection Procedure

The validated questionnaires were distributed to a group of respondents in the selected Commercial bank of Ethiopia departments. Using the self-completion technique also gives participants the chance to fill out the questionnaire at their convenience, in their own time, and to adequately

answer all the questions on the research instrument (Creswell, 2013). The questionnaires were then retrieved from the participants through personal contact for sorting and data analysis.

3.5. Data Analysis

To a position to pick the fantastic approach of analysis, the level of measurement understood. For each type of measurement, there was an appropriate method applied. Descriptive statistics were used to examine the data gained from the questionnaires by respondents. Data were analyzed using statistical techniques, particularly percentages, percentage averages, mean and standard deviation.

3.6. Validity and Reliability of the Research

The questionnaire was once authenticated by using the potential of a pilot administration to a pattern of some chosen respondents. Any inconsistency determined was once due to this fact corrected and subsequently administered to the goal sample. A reliability check was once additionally performed in the study According to Pallant (2013).

In addition, to make sure the research‘s reliability of questioner the researcher conducted Cronbach's Alpha reliability test by using SPSS (Statistical Package for the Social Sciences) and found that 0.734 Cronbach's Alpha for the overall questionnaire for the role of NG|Screener fraud prevention. It was generally considered acceptable s, suggesting that the items have relatively high internal consistency.

Table 3.2 Reliability Result Items	**Cronbach’s alpha coefficient**	
Control environment	6	0.732
Risk Assessment	6	0.768
Control activities	6	0.729
Information and communications	5	0.750
Monitoring activities	6	0.728
Fraud challenge	10	0.713
Investigation	5	0.719

Table 3.1 Reliability Result

3.7. Ethics and Code of conduct

The researcher places due care in accumulating and inspecting statistics as a capacity to guarantee the accuracy of results. The researcher additionally maintains the confidentiality of the respondents. In line with this, the researcher does now not analyze the data that contradicts the reflection of the respondents. They are given the chance to ask anything about the study and were informed and made free to refuse or stop the questionnaire or interview at any moment they want if that was their choice.

CHAPTER FOUR: DATA ANALYSIS AND INTERPRETATION

Introduction

This chapter deals with the presentation of data, analysis, and interpretation. To collect the data and extract findings, a questionnaire was prepared and distributed to employees of the selected commercial bank of Ethiopia departments.

This chapter presents the findings of the research in accordance with the research objectives. The analyses and interpretation of the data collected from the respondents were resented. It began with a description of the demographic and general characteristics of the participating respondents. The study discussed the evaluation of NG|Screener role in fraud prevention in mitigating the challenges in the banking systems, the effectiveness of the system in the internal control system components variables (control environment, control activity, Information and communication, monitoring activity, and risk assessments), and the relevance of the system in banking internal control improvements area in preventing fraud risk by using descriptive statistics.

The chapter also provides the interpretation of the results of the data derived from 45 respondents within the Commercial Bank of Ethiopia. Forty-five questionnaires were prepared and distributed to managers, Senior CBE IT staffs; Audits, and control departments, and 45 questionnaires were returned and responded. The realized response rate was therefore 100% and was considered to be excellent.

The analysis was undertaken through descriptive statistics and the study findings are presented in the form of mean value, frequency, percentage and standard deviation. The discussion of the outcome is performed on the basis of the output obtained from Statistical Package for Social Sciences (SPSS) version 20. The questionnaire was developed by using a 5 point Likert rating scale (from 1 to 5); where 1 denoted Strongly Disagree, 2 Disagree, 3 Neutral, 4 Agree and 5 Strongly Agree for all questions on the evaluation of NG|Screener system.

4.1. Demographic Information of the respondents.

This section presents the general information of the respondents including gender, age, level of education, and duration of service in the bank.

Characteristics	Responses	Count	Percentage
sex	Male	33	73.3
	Female	12	26.7
	Total	45	100
Age	26-35	19	42.2
	36-45	23	51.1
	46-55	3	6.7
	Total	45	100
Position of respondents	Manager	2	4.5
	Team Leader	6	13.3
	Senior Application analyst	10	22.2
	Application analyst	7	15.6
	Senior IT auditor	5	11.1
	Senior quality management and control officer	6	13.3
	quality management and control officer	1	2.2
	Senior server administrator	2	4.5
	Senior fraud investigation officer	5	11.1
	System Engineer	1	2.2
	Total	45	100
Educational Level	Degree	33	73.3
	Masters and above	12	26.7
	Total	45	100
Year of experience	1-5 years	2	4.4
	6-10years	20	44.4
	11-15 years	17	37.9
	Above 15 years	6	13.3
	Total	45	100

Source: Own survey, 2022

Table 4.1. Demographic characteristics in general.

As the data obtained from the respondents, 73.3% of the respondents are male and 26.7% are female. Concerning the age of the respondents, 42.2% of the respondents are in the age range 26-35, while 51.1% of them are in the age range 36-45 , and the remaining 6.7% are in the age range 46-55. In regards to the level of respondent qualifications, 73.3% of the respondents have their first degree, and 26.7% have a Master's degree.

Regarding respondents' job positions almost all respondents are in senior and managerial positions in a different banking environment and are experienced in the research study areas. The composition of positions in application, server, audit, and fraud investigation areas of the bank.

Furthermore, the Experience results pointed out that 4.4% of the respondents had served between 1-5 years, 44.4% had served between 6-10 years, and 37.9% of the respondents had served 11-15 years while 13.3% had served above 15 years. From the finding of the study, it can be said that most of the respondents had served the bank for a period of more than 5 years, which is considered to give the bank a better competitive advantage since the employees has well experience in banking service. This further affirmed that the respondents were well-positioned to respond correctly to queries relating to NG| Screeners role in fraud prevention based on the experience gained in the bank.

4.2. NG|Screener fraud prevention role on internal fraud challenge.

The first objective of the study was to evaluate the role of the NG|Screener project implementation on fraud prevention in commercial banks of Ethiopia. The questionnaire was designed based on the challenge of internal fraud types to assess the role of NG|Screener in fraud prevention challenges.

To achieve this objective respondents were requested to indicate their level of agreement on the questionnaire items on the subject. The responses were ranked on a five-point Likert scale where: 1= strongly disagree; 2= disagree; 3= neutral; 4= agree; and 5= strongly agree.

As shown in table 4.2 the role of the project in fraud prevention of the challenges on core applications in the commercial bank of Ethiopia respondent agreement on the detection, identification, and prevention of fraud ranges from 66% to 100%, meaning the role of NG|Screener is a great impact on mitigation the banking internal challenges across the application.

NG|Screener Fraud prevention on Core application fraud challenges	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
Identify Transaction Reversal and deletion	Frequency		1	1	21	22	45	4.42	.657
	Percentage	0	2	2	47	49	100		
Detect Forgeries and falsification of documents	Frequency	1	3	11	15	15	45	3.89	1.027
	Percentage	2	7	24	33	33	100		
Identify Fraudulent money transfers and withdrawal	Frequency				29	16	45	4.36	.484
	Percentage	0	0	0	64	36	100		
Control Abuse of Administrator Privileges	Frequency			3	21	21	45	4.40	.618
	Percentage	0	0	6	47	47	100		
Identify Account and Customer-opening fraud (opening with fake identification)	Frequency	2	1	12	19	11	45	3.80	.991
	Percentage	4	2	27	42	24	100		
Mitigate Unauthorized Withdrawals	Frequency	2		1	21	21	45	4.31	.900
	Percentage	4	0	2	47	47	100		
Monitor and prevent Unauthorized use of back end privileges	Frequency	1	2	5	22	15	45	4.07	.915
	Percentage	2	4	11	49	33	100		
Find out loopholes and analysis on systems and applications	Frequency		2	9	20	14	45	4.02	.839
	Percentage	0	4	20	44	31	100		
Identify Four Eyes Violation on transactions	Frequency			9	19	17	45	4.18	.747
	Percentage	0	0	20	42	38	100		
Identify Theft of confidential information of customers	Frequency			4	25	16	45	4.27	.618
	Percentage	0	0	9	55	36	100		
Group Mean and Standard Deviation								4.17	0.78

Table 4.2 Role of NG|Screener project fraud prevention in internal fraud challenges.

Source: Own Survey, 2022 SPSS version 20 outputs, Note: 1 = strongly Disagree, 2 = Disagree, 3 = neutral, 4 = Agree, 5 = strongly Agree

From the analysis shown in this table on the role of the system in the prevention of fraud of core application challenges identified from the table are;

The first question raised to the respondents was NG|Screener role in the identification of transaction reversal and deletion for fraud prevention. Around 96% of the respondents agreed and strongly agreed that there was an important system in the identification of misused transaction reversal and deletion, while 2 % of them were undecided about it. While the remaining responded equally with 2% disagreed. The finding shows that by using the system a better identification is performed on identifying the transaction reversal and deletion.

In the second question, the survey participants were asked NG|Screener role on Detect Forgeries and falsification of documents. In this respect, 24% were undecided, however, the majority of them (66%) agreed and strongly agreed. Moreover, the mean response obtained in this regard was 3.89 implying that the use of NG|Screener system helped the company to a high extent. Because by using the system they can detect anomalies. From the response to this benefit, the finding is that the system can bring the reduction of falsification documents provided by the company.

In the third issue, participants were asked were the role of the system in Identify Fraudulent money transfers and withdrawals. 36% strongly agreed and 64% agreed on the specified benefit of NG|screener System. From the result, we can conclude that the NG|Screener system can make changes in the controlling of any transfers and withdrawals in the bank.

The fourth question asked to respondents related to the role of NG|Screener was control abuse of administrative privileges. The majority of the study participants (94%) agreed and strongly agreed that using NG system can control system administrators. Meanwhile, close to 6% of them were neutral. This shows that NG|Screener system has indeed been used in the monitoring and controlling of misused privileges in the reduction of system abuse.

In the evaluation some respondents have reflected their disagreement in identifying account and customer opening fraud, Mitigate Unauthorized Withdrawals, monitoring and preventing unauthorized use of back end privileges, Detect Forgeries and falsification of documents and find out loophole analysis 6%, 4%, 6%, 9%, and 4% respectively and agree the system has a great positive impact in mitigating issues 66%, 94%, 82%,66%, and 75% respectively on the evaluation of the system in the prevention of fraud in the bank.

For the last role of NG|Screener role on Identify Theft of confidential information of customers 36% strongly agreed and 55% agreed while 9% of them were neutral with a mean value of 4.27.

From the response, we can conclude that this benefit can be achieved with an argument that it comes from the availability of the fraud prevention system.

4.3. Role of NG|Screener relevance in internal control system Improvement areas.

The secondary objective of the study was to assess the relevance of the NG|Screener system's role in internal control improvement through commercial banks of Ethiopia. To do this the respondents were requested to indicate their level of agreement on the system's role in internal control improvement in the bank's internal system controlling and monitoring areas.

The responses were rated on a five-point Likert scale where: 5 = strongly agree; 4 = agree; 3 = Neutral; 2 = disagree and 1 = strongly disagree. The mean and standard deviations were generated and presented in Table 4.3.

NG|Screener Fraud prevention on internal control improvement area	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
Improve cyber security of the bank activity	Frequency			5	25	15	45	4.22	.636
	Percentage	0	0	11	56	33	100		
Great role on build strong management control and Provide continuous input.	Frequency		1	3	21	20	45	4.33	.707
	Percentage	0	2	7	47	44	100		
Increase internal audit performance.	Frequency			1	19	25	45	4.53	.548
	Percentage	0	0	2	42	56	100		
Enhance the bank line of defense on internal control system.	Frequency			1	28	16	45	4.33	.522
	Percentage	0	0	2	62	36	100		
Influence to prepare fraud Controls Policy and procedure	Frequency		1	5	17	22	45	4.33	.769
	Percentage	0	2	11	38	49	100		
Group Mean and Standard Deviation								4.35	0.64

Source: Own survey, 2022 *Table 4.3 Role of NG|Screener project on CBE internal control improvement.*

The findings in Table 4.3 show that due to the implementation NG|Screener project implementation the respondents indicated that their bank improve internal control systems, policy, and procedures. As depicted in table 4.3, the improvement analysis respondents agreement in percentage in the following areas,

For the first role of NG|Screener on internal control fraud prevention area on improve cyber security of the bank activity. 89% of the respondents agreed and strongly agreed that there was an increase in improvement of the internal cyber security on core system areas in the bank, while 11% of them were undecided about it there was no participant who responded disagreed and strongly disagreed. The finding form this result and interviewees show that using NG|Screener allows the bank to improve the internal cyber control and enhancement.

The second question asked was NG|Screener in the role of building strong management control and providing continuous input. In this respect, 7% were undecided, however, the majority of them (91%) agreed and strongly agreed. Moreover, the mean response obtained in this regard was 4.33 implying that the company has achieved or experienced this benefit from the system. From the response to this role, the finding shows that an internal control system is necessary and important in the bank to build strong management control.

In the third role in internal control improvement to increase internal audit performance, participants were asked if there were improvements in of internal audit processes. 56% strongly agreed and 42% agreed on audit process improvement by the system, while 2% of them were neutral. The result shows that no participants disagreed or strongly disagreed on the role of system regarding improved efficiency of internal audit processes. From the result and interviewees' responses, we can conclude that the systems can improve internal audit performance.

The fourth question asked respondents related to the system's role in enhancing the bank's line of defense internally. The majority of the study participants (98%) agreed and strongly agreed that using NG|Screener System enhances the bank's line of defense against fraud through the company. Meanwhile, 2% of them were not sure about this role. This shows that NG|screener system could be the key to improving the bank line of defense.

The last role requested respondents to answer the influence of NG|Screener role on preparing fraud Controls Policy and procedure. The respondents' comments on the questionnaire, before implementing the bank have no fraud policy. But after the project was implemented the bank prepared fraud Controls Policy and procedure. The majority of the study participants (89%) agreed and strongly agreed that using NG|Screener System enforces the banks to prepare policy and procedures. while 11% of them were not sure about this role. and 2% disagreed This shows that NG|Screener system could be the key in the continual fraud policy and procedure enhancement.

4.4. NG|Screener system Effectiveness through internal control systems components (IC's).

The other objective of the study was to evaluate the role of the NG|Screener project implementation on fraud prevention effectiveness in the internal control system components as per the COSO framework. The questionnaire was designed based on the banking environments to assess the role of NG|Screener in the control areas.

To achieve this objective respondents are requested to indicate their level of agreement on the questionnaire items on the subject. The responses were ranked on a five-point Likert scale where: 1= strongly disagree; 2= disagree; 3= neutral; 4= agree; and 5= strongly agree.

4.4.1. Control Environment

This part of the study sought to evaluate the effectiveness NG|dcreener system role on control environment in the commercial bank of Ethiopia. The results showed that it must be emphasized that all the items reported under the control environment had mean scores between 3.73 and 4.20. This means that the majority of the respondents were of the view that NG|Screener system role in the control environment component of the internal control systems is effective. The overall mean of the control environment can be approximated to 4.05 which indicates an agreement in practices of the control environment but room for improvement.

The highest mean 4.20 indicates that the majority of respondents agreed that the system used for the establishment of fraud risk policy and procedures and control of all processes, branches, and business areas. This indicates internal control system has an important role in the bank for fraud prevention and protection of the bank and the customer.

In the role of NG|Screener in the internal control system, the system is powerful to control fraud risk in server application and database areas with the respondent's mean value of 3.98 agreed on the system role. But in the 17.8 percent of the respondents were neutral and 2.2% responded and disagreed with the role in the area. This indicates there is a gap in the respondent's understanding and Knowledge of these areas of the system.

The result of the survey is also management establish controls appropriately documented and explained which is indicated by the mean value of 3.73. This means the majority of the respondents agreed that the management established controls appropriately documents, investigated by Ng|screener system. As compared to others majority of the respondents are neutral in evaluating this variable which was 28.9% neutral.

Statement on Control Environment	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
NG|Screener is powerfully internal control of servers, applications and database environment	Frequency		1	8	27	9	45	3.98	0.69
	Percentage		2.2	17.8	60	20	100		
The bank establish NG|Screener fraud risk prevention, detection and mitigation policies and procedure in the control environment	Frequency			8	20	17	45	4.20	0.73
	Percentage			17.8	44.4	37.8	100		
NG|Screener fraud risk detection and mitigation internal control systems decrease the frauds in the bank internal environment	Frequency		1	4	27	13	45	4.16	0.67
	Percentage		2.2	8.9	60	28.9	100		
Are management overrides of established controls appropriately documented, explained, and are deviations from such controls investigated by NG|Screener?	Frequency		3	13	22	7	45	3.73	0.81
	Percentage		6.7	28.9	48.9	15.5	100		
Is NG|Screener in CBE has a very sound control environment to safeguard systems against abuse?	Frequency		1	7	27	10	45	4.02	0.69
	Percentage		2.2	15.6	60	22.2	100		
NG|Screener system are control process, branch and district business and IT accomplishments on core systems environments.	Frequency		1	4	25	15	45	4.20	0.69
	Percentage		2.2	8.9	55.6	33.3	100		
Group Mean and Standard Deviation								4.05	0.71

Source: own survey, 2022

Table 4.4. Control Environment

4.4.2. Risk Assessment

Risk assessments become an integral part of the internal control system. The management is responsible to identify and assess control risk caused by failure of internal control. There should be strategies for identifying Risk, and systems to respond to risk and reduce the risk. The survey results on the role of NG|Screener fraud prevention system on the risk assessment are presented as follows. This variable was investigated to find out how the NG|Screener system is effective in the banking sector for identity, analyzing, and managing risk that is related to the overall bank operation activity.

From the table, it shows that NG|screener has an important role in the risk assessment of the bank, and there exists an appropriate strategy for identifying risks. The banks have made some improvements on risk response to offer an appropriate response to the risk mean value of 3.91 which was 28.9% of respondents are neutral in their response. Overall the role of NG|Screener effectiveness in risk assessment can be approximated to a mean of 4.07 which shows there is an effective risk assessment on ICs commercial bank of Ethiopia.

Statement on Risk assessment	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
The role of system has an appropriate strategy of identifying the bank fraud risks internal control risk assessment.	Frequency			4	31	10	45	4.13	0.548
	Percentage			8.9	68.9	22.2	100		
The control system/technology is able to identify the location and the performers to assess the fraud risk related activities	Frequency			7	23	15	45	4.18	0.684
	Percentage			15.6	51.1	33.3	100		
NG|Screener provide bank risk valuation based on violation risk conditions using activities.	Frequency			8	24	13	45	4.11	0.682
	Percentage			17.8	53.3	28.9	100		
NG|Screener periodically identifies internal factors, which could cause financial and IT systems fraud (Risk identification).	Frequency		1	9	21	14	45	4.04	0.852
	Percentage		2.2	20	46.7	31.1	100		
NG|Screener in CBE report risk issues when they appear and treat them comprehensively (Risk response).	Frequency			13	23	9	45	3.91	0.701
	Percentage			28.9	51.1	20	100		
The system is powerful to assess risk causes and the likelihood of the risk occurrence (Risk evaluation).	Frequency		1	6	28	10	45	4.02	0.753
	Percentage		2.2	13.4	62.2	22.2	100		
Group Mean and Standard Deviation								4.07	0.70

Source: own survey, 2022 *Table 4.5. Risk Assessment*

4.4.3. Control Activities

From the components of the internal control system: NG|Screener internal control system can detect and mitigate every area of fraud risk and other illegal activities (Mean 3.71 and SD .843) It implies that respondents agreed since the mean value is higher than 3.41. The survey result shows that respondents agreed that the NG|Screener role in identifying the errors that leads to misrepresentations in the financial reports the mean value is 4.22. As indicated in the result table,

NG|Screener captures all core system operational and IT activities for controlling each occasion of activities Control the mean value is 4.11 which lay on agree rang.

From the descriptive statistics result the system contributes to management selects and developing control activities that are designed and implemented to restrict technology access rights, and alert identified fraud risks to authorized users to protect mean value 4.22. The Overall mean of the control activities for the six questions can be estimated to 4.10 which is the respondent are in agreement about the role of NG|Screener effectiveness on control activity in the bank.

Statement on Control activities	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
NG|Screener internal control system can detect and mitigate every areas of fraud risk and other illegal activities.	Frequency		6	6	28	5	45	3.71	0.843
	Percentage		13.3	13.3	62.2	11.1	100		
The system identify the errors that leads to misrepresentations in the financial reports.	Frequency		1	5	22	17	45	4.22	0.735
	Percentage		2.2	11.1	48.9	37.8	100		
The system captures all core system operational and IT activities for controlling each occasion of activities Control.	Frequency		2	6	22	15	45	4.11	0.804
	Percentage		4.4	13.3	48.9	33.3	100		
NG|Screener system in the bank has control over its employee activity and records	Frequency		3	1	24	17	45	4.22	0.795
	Percentage		6.7	2.2	53.3	37.8	100		
System Management control activities consider all the relevant core systems business processes, information technology and locations where control activities are needed.	Frequency			8	25	12	45	4.09	0.668
	Percentage			17.8	55.5	26.7	100		
The system contributes to management selects and develops control activities that are designed and implemented to restrict technology access rights, alert identified fraud risk to authorized users to protect.	Frequency		1	4	24	16	45	4.22	0.704
	Percentage		2.2	8.9	53.3	35.6	100		
Group Mean and Standard Deviation								4.10	0.76

Source: own survey, 2022

Table 4.6. Control Activities

4.4.4. Information and communication

Table 4.7 shows that respondents have agreed NG|Screener system had important in fraud prevention that NG|Screener provides collected Control information‘s data are communicated to the management staff indicates a mean of 4.07 and the system collected Transactions and employee data activities and classified to provide reliable information. (Mean 4.38 and SD .65). The system share illegal activities control reports to the accountable organ to handle the concerns in fraud (Mean 4.2 and SD 0.625): The result shows that respondents were answered neutral or indifferent about the items which measure 11.1%. The result shows that respondents were agreed on NG|Screener produces reports that contain operational, financial, customer, non-financial and compliance-related information about core system operations (Mean 4.24 and SD .712). This implies that there is a good effect in communication fraud and the risk of communicating the effects of fraud in the banking industries to concerned bodies. Overall the result shows that information and communication are an effective indicator of information on fraud prevention in commercial bank of Ethiopia. The respondents also agreed on the system has effective automatic reporting processes in communicating to all process, branch, and district responsible authorities in CBE of the system identified frauds indicates a mean of 4.02.

The study findings indicated that established systems that carried out that information and communication which leads fraud activities to the responsible management in the banks led to increased fraud prevention in the commercial banks and the highest application was on enhancing quality fraud risk controlling.

Statement on Information & communication	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
NG|Screener provide collected Control information's data are communicated to the management staffs.	Frequency			7	28	10	45	4.07	0.618
	Percentage			15.6	62.2	22.2	100		
The system collected Transactions and employee data activities and classified to provide reliable information.	Frequency			4	20	21	45	4.38	0.65
	Percentage			8.9	44.4	46.7	100		
The system share to illegal activities control reports to the accountable organ to handle the concerns in fraud.	Frequency			5	26	14	45	4.2	0.625
	Percentage			11.1	57.8	31.1	100		
NG|Screener produce reports that contain operational, financial, customer and non-financial and compliance-related information about core system operations	Frequency		1	4	23	17	45	4.24	0.712
	Percentage		2.2	8.9	51.1	37.8	100		
The system has effective automatic reporting processes in communicating to all process, branch and district responsible authority in CBE.	Frequency		1	9	23	12	45	4.02	0.753
	Percentage		2.2	20	51.1	26.7	100		
Group Mean and Standard Deviation								4.18	0.67

Source: own survey, 2022 *Table 4.7. Information and Communication*

4.4.5. Monitoring activities

The descriptive statistics in Table 4.8 gives the percentage, mean, and standard deviation value of the study variables. The bank has monitoring activities in relation to operational activities, Monitoring the internal control system of the bank is important to achieve the bank objectives, NG|Screener system role on Monitoring helps to determine whether controls under the bank are effective and Internal control monitoring activities of the bank could reduce the occurrence of fraud and illegal activities. The majority of the mean value for each specific question was above 4.09 except for one question.

From the result, table Is NG|Screener fraud prevention tool is AI and machine learning monitoring behavioral and activity analysis? (Mean 3.24 and SD 0.981): This shows that respondents disagreed that NG|Screener did not use AI and machine learning based on the finding of the evaluation of the internal control system. The overall grand mean value 4.00 shows that all items of the evaluation of the role of NG|Screener on monitoring activities are effective in fraud prevention in the commercial bank of Ethiopia.

The study found that all components are relevant to each objectives fraud prevention category. When looking at any monitoring activities are effective in making operations effective and efficient.

Statement on Monitoring activities	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
NG|Screener monitors core system business and IT environments to achieve the bank objectives in fraud detection and mitigation.	Frequency		2	3	29	11	45	4.09	0.701
	Percentage		4.4	6.6	64.4	24.4	100		
NG|Screener monitoring dashboard could reduce the occurrence of fraud risk activities.	Frequency			4	19	22	45	4.4	0.654
	Percentage			8.9	42.2	48.9	100		
System provides visualization dashboard of real time data and back history activity data to all management controls staffs.	Frequency	1		5	26	13	45	4.11	0.775
	Percentage	2.2		11.1	57.8	28.9	100		
System in the bank provides data to reviews employee performance activity monitoring based on the assignee level.	Frequency	1	1	7	20	16	45	4.09	0.9
	Percentage	2.2	2.2	15.6	44.4	35.6	100		
Internal audit identifies and make auditing activity using System data provides and periodically to ensure compliance	Frequency		1	4	30	10	45	4.09	0.633
	Percentage		2.2	8.9	66.7	22.2	100		
Is NG|Screener fraud prevention tool is AI and machine learning monitoring behavioral and activity analysis?	Frequency	2	5	24	8	6	45	3.24	0.981
	Percentage	4.44	11.1	53.33	17.8	13.33	100		
Group Mean and Standard Deviation								4.00	0.77

Source: own survey, 2022 *Table 4.7. Monitoring Activities*

4.4.6. Overall NG|Screener system Effectiveness through internal control systems components (IC's).

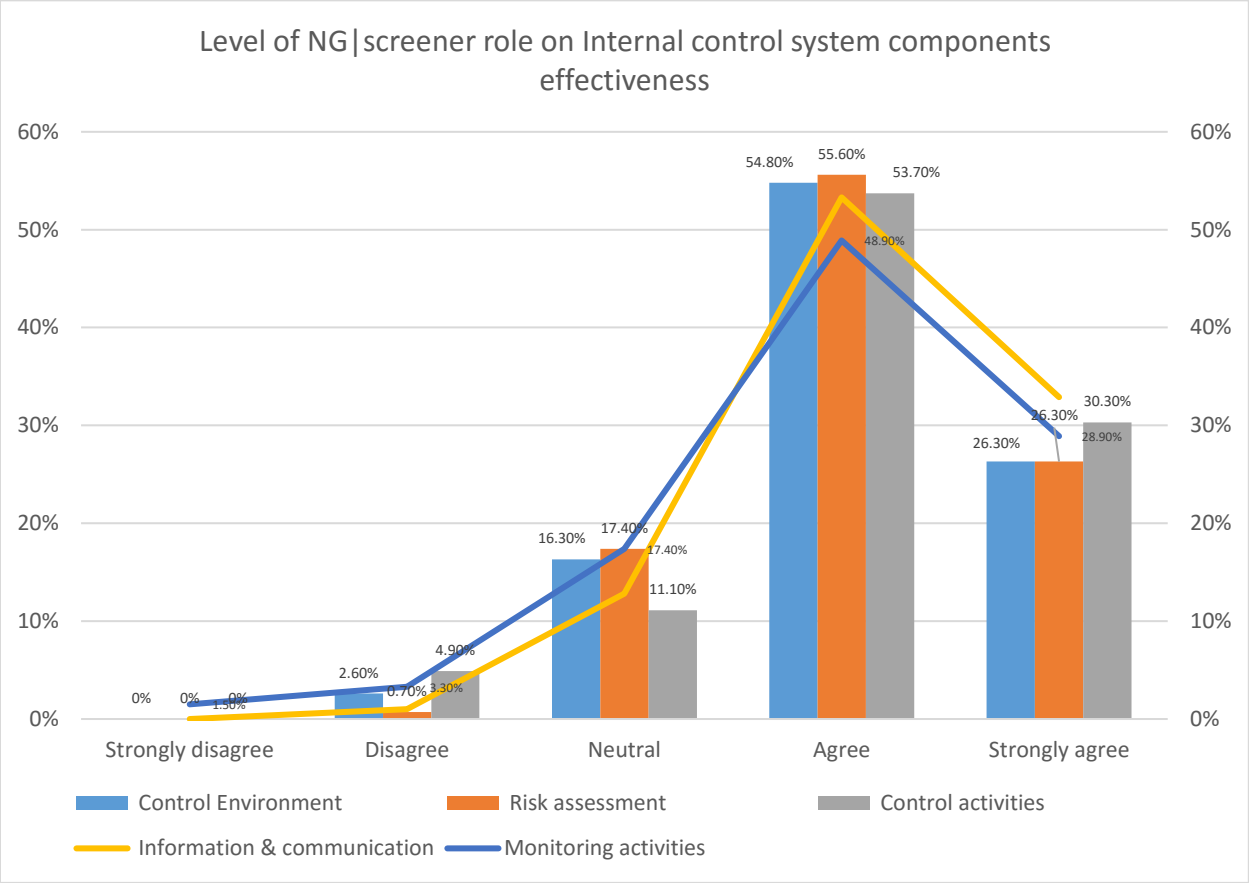

Figure 4.1: overall Effectiveness of NG|Screener role in internal control system components.

Figure 4.1 shows the overall agreement of the respondents who agreed above 48.9% for all control components and strongly agreed 26.30% as shown in the figure. The finding from the respondents shows NG|Screener project implementation is effective in the IC's components in the reduction and fraud prevention by control and analysis of environments.

- Control environment-based on the findings of respondents the system is a powerful technology to control banking system environments including servers, databases and

applications servers with the access each end areas in the head office, district, branch areas to safeguard the environment from abuse and frauds.

- Risk assessment- as per the respondents risk assessed using the internal control systems and they agreed on the system provides to assess the behaviors of the employee as well as the system functionality with each areas in the identification of loophole and works as per the policy and procedures in the core system areas.
- Monitoring and controlling activities-the respondents agreed on the system monitor and control activities in the core systems 77.8% and 86% respectively. This shows NG|Screener system is the vital role in the banking industry to control activities in the bank and monitoring each performers to reconciled and managing based on the job descriptions to handle illegal activities and measurement.
- The other important findings in information and communication of the system based on the respondents, 86% agreed on the system providing collected information, transactional activates, employee activities to the respective process/branches. In addition to this the system provides control reports automatically distribute to the responsible person to handle the fraud and prevent corrective action on the identified fraud risks.

4.1. Role of the NG|Screener system in investigating fraud and risk activity control.

Fraud investigation is the other objective of the study. 68% of fraud cases occur within organizations by employers and employees, with the rest externally by those in the value chain (KPMG, 2014). In this evaluation of the role of the NG|Screener project implementation on fraud prevention, commercial banks of Ethiopia greatly benefited in the investigation based on the system data, and fraud investigation and controlling areas have strongly enhanced the performance of analyzing data through the bank and customer complaining request. The questionnaire was

designed based on the investigation parametric for fraud cause and the respondent's agreement on the system's role is shown in table 4.4.

	NG|Screener investigation role of fraud risk	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
1	The system provides accurate and reliable fraud data for compliance and law court.	0	2%	4%	73%	20%
2	The system captures a long period of data for investigation from back history.	0	2%	13%	31%	53%
3	The system identifies the fraud risk in quality data with a minimum time frame.	0	0	17%	47%	36%
4	The system provides data for anti-corruption and the legal cause of fraud.	0	2%	11%	58%	29%
5	Provides the capability of management staff to investigate cases at the starting point.	0	2%	4%	60%	33%
6	The system has the capability to identify the root causes of internal fraud risk loopholes in the core systems areas.	0	2%	4%	73%	20%

Source: Own survey, 2022 *Table 4.8. Role of NG|Screener investigation in the bank*

The overall role of the system in investigation are positive impact over the bank and over 83% agreed on the evaluation questions. The analysis shows the following responses;

- 93% responded "agree" that the system provides accurate and reliable fraud data for compliance and law court while 2% "disagree".
- 84% responded "agree" The system captures a long period of data for investigation from back history in the cause of back investigation.
- Based on the respondents, the system identifies the fraud risk in quality data within a minimum time frame of 83% of the respondents.
- 87% responded "agree" that the system provided data in the investigation of legal evidence and compliance causes the core servers and applications.

4.2. NG|Screener in fraud prevention

System fraud prevention objective is the dependent variable of this research work and the bank invest in huge cost to deploy the system. Based on the evaluation showed in table 4.5, the

respondents agreed the system provides fraud prevention role in the banks based on the respondents agreed level above 82.22%.

Statement on NG|Screener in fraud prevention	Category	Level of agreement					Total	Mean	SD
		1	2	3	4	5			
The bank able to establish fraud prevention policies	Frequency		2	6	17	20	45	4.22	.850
	Percentage		4.44	13.33	37.8	44.4	100		
System fraud prevention capability improve internal control system area exhaustive	Frequency		1	4	16	24	45	4.36	.773
	Percentage		2.2	8.9	35.6	53.3	100		
System is computerized fraud prevention methods	Frequency		2	5	15	23	45	4.31	.848
	Percentage		4.44	11.14	33.33	51.11	100		
The possibility of fraud occurrence is reduced by means of NG|Screener fraud prevention system.	Frequency			5	18	22	45	4.38	.684
	Percentage			11.1	40	48.9	100		
Group Mean and Standard Deviation								4.32	0.789

Source: Own survey, 2022 *Table 4.5. NG|Screener in fraud prevention*

The Table 4.5 gives the percentage value of the study variables. The mean the bank able to establish fraud prevention policies as shown by the 82.22% which indicated respondents were agreed, System fraud prevention capability to improves internal control system area exhaustive respondents were agreed over 88.88% this means the evaluation result indicates the bank internal control is supported by the system fraud prevention tools.

As the result clearly shows respondents agreed on the system is computerized fraud prevention methods since they agreed the percentage cumulative value 84.44%: This result implies banks are trying to use modern computerized technologies to enhance monitoring and controlling activities in the bank.

The respondents agreed 88.89% on the possibility of fraud occurrence is reduced by means of NG|Screener fraud prevention system. Based on the overall respondent agreed on the system fraud prevention on the bank activities the system provides by examining internal control systems and provide input to enhancement areas in the bank.

The finding of the study NG|Screener fraud prevention contribute to better role by the banking and financial institutions. The system able to prevent the frequent occurrence of fraud. Banks should have in place a comprehensive internal control management process to identify; measure, monitor

and control internal control system effectiveness and compliance. The finding of the study also supported system fraud prevention measures were found to be in place and the study concluded that a significant and positive relationship exists between Internal Controls and system/technology fraud prevention in banks.

4.3. Comments from Questionnaire's Respondent

Comments were obtained through open paragraph questions at the end of the questionnaires are listed below on the recommendation.

- Giving NG|Screener training for controllers has a great contribution to bank fraud prevention and fraud awareness success.
- Since the Bank currently is not benefiting from the system as intended; it should enforce the implementation of the system.
- It has to be knowledge-based and common understanding must be there in the bank to manipulate the system fraud prevention.
- Implementing maximum risk prevention tools and holistic use in the bank to compact fraud risk.

CHAPTER FIVE: Summary, Conclusion, and Recommendation

In this section of the paper, the researcher sets the objectives of identifying the role of NG|Screener project on fraud prevention in CBE and stating the recommendations based on the evaluation data analysis and forwarding recommendations based on findings. This chapter provides the conclusion to the study and forwards recommendations

5.1. Summary of the major findings

The purpose of this study was to evaluate the role of NG|Screener project on fraud prevention in the Commercial Bank of Ethiopia. Therefore, the Self-administered questionnaires designed for forty-five respondents were distributed to collect the primary data. All these data collection instruments were used to assess the role of the project in fraud risk challenges, the relevance of the system in internal control improvement areas, and the system's impact on the internal control system components (control environment, risk assessment, control activities, information communication, and monitoring activities area). The approach used in this study was a quantitative research approach that used a descriptive type of research. According to analysis and findings from data sources in chapter four, the following major evaluation results of NG|screener role in fraud prevention were identified and summarized. The following major findings of evaluation associated with each research question and objectives were identified. In the banking industry, one of the challenges frequently occurred is fraud. This highly affects commercial banks of Ethiopia in the finance industry and customer integrity. NG|Screener project implementation focused on which was related fraud challenges, Fraud investigation, internal control system enhancement, and internal control component components challenges. Therefore, the summary of major findings was described in accordance with each evaluation question.

- Internal frauds occurred mainly by system issues and internal control system weakness across the bank. The researcher identified the role of NG|Screener system as highly relevant in the identification of loopholes, decreasing fraud, and identifying the fraud causes. In addition to this, the role of the system had great in the mitigation and identified the fraud risk challenges that happened and triggered fraud trials across the bank environment. Furthermore, the system applied to internal fraud challenges is reduced using technological fraud prevention methods.
- The impact of NG|Screener project on the strength of the internal control system in cyber security, internal audit, and others to handle every threat on CBE networks core activity is

actively managed and controlled. On the other side, the role of the system provides an integrated strong line of defense across the system, management, and organizational activity. The other thing is the system that has a positive impact on the amendment, development, and frequent reviewing of policy, and standard operating procedure in the bank system.

- The fraud caused happed highly integrated into the bank environment systems and the system used in the analysis of identification fraudsters in the cause of compliance and legal justifications in the internal and external environments employee and customer.
- In the banking industry, the internal control system environment in using systems or technology and other policy and procedures is one of the core areas of fraud risk prevention for the current globalization world to protect the business environment.
- Internal controls system like NG|Screener technological system is important to enhance the internal control systems both in systematically and other policy, procedures will be strong bonding to create strong fraud prevention in the banking and financial institution.
- In the banking system, all the environments, activities, and communication must be managed and controlled to handle any causes in the bank and protect customers from fraudsters as well as the growth of the organization to be competitive around the globe.
- The bank did not cover all environments in the banking system to protect customers and employees from fraud risk prevention only focused on the core application and server environments.

5.2. Conclusion

The cause or the starting point of fraud risks is a weakness of the internal control system. In order to handle this weakness, different mechanisms will be developed and implemented. Commercial bank of Ethiopia uses NG|Screener fraud prevention technology as a strategy for fraud risk management in the bank. This provided an opportunity to make continuous improvements in the area and enables the bank to maintain or enhance competitiveness by safeguarding the internal and external environments and customers. By adopted the technology of NG|Screener, the bank was beneficiary of improvement in productivity, decreasing the chance of fraudulent activity, improved the effectiveness of controlling and monitoring internal control systems, and efficiency of doing banking activity including transactions. Therefore, based on the above summary of the major findings and categorized respective to each research question, it can be concluded that the following basic evaluation criteria role of NG|Screener in fraud prevention evaluations.

- Effectiveness- NG|Screener achieved its objective by monitoring activities, controlling activities, controlling environments, risk assessments, and communicating relevant information across the banking environment.
- Relevance- NG project supports the bank by identifying the weakness of systems and improving the loophole areas by sniffing data in the background areas. Also, add value to the management to manage the employee's behavioral analysis and control risk at the spot by improved the bank's internal control system areas.
- Impact- the implementation of NG|Screener project contributes a positive impact on the bank in the reduction of core systems fraud risk challenges across the organization environment.
- Efficiency – the project is highly efficient in fraud prevention based on the data analysis in chapter 4 in banking systems.

5.3. Recommendations

Based on the study findings, the following recommendations are in sight;

- The banks should improve the fraud risk policy based on technological change and fraud risk challenges by continuously reviewing internal and external bank control environments.
- The bank should give more emphasis on improving fraud risk prevention 360^0 using internal control systems and move to machine learning and artificial intelligence systems for identifying red flak risks and blocking the cause immediately using the risk score or matrix.
- Risk management is the key area in fraud analysis. Therefore the bank will build a strong department as well as implement risk management systems both by technical and academic capability to trigger risk register and profiling fraud risk management.
- Banking Sustainability - fraud metrics are frequently changed in the world. Therefore protecting fraud is one of the sustainability of existence in the banking industry. CBE will enhance the systems and use technology to handle fraud causes and accomplish the mission and vision.
- The bank provides massive training for internal control management including risk identification, fraud prevention, and detection, and identifying issues and resolutions.
- The other recommendation of this study is that the bank should enhance the level of internal audit capacity and management skills for system manipulation that has a direct impact on

the fraud risk prevention performance and success that will improve the speed and quality of services, as well as improves the competitiveness of the Commercial Bank of Ethiopia on the Ethiopian banking industry.

5.4. Suggestions for Future Work

- ✓ The role of Artificial intelligence and machine learning technology in fraud detection and prevention in Ethiopian banking and financial industry.

References

Aziz, S. and Dowling, M. (2018). Machine Learning and AI for Risk Management. *Disrupting Finance*, pp.33-50.

Basel Committee on Banking Supervision, Principles for Enhancing Corporate Governance, Principle 6. See also OECD Steering Committee on Corporate Governance, Corporate governance and the financial crisis, 15.

Basel Committee on Banking Supervision, Principles for Enhancing Corporate Governance, Principle 7.

Rahman, R.A. and Anwar, I.S.K. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. Procedia - Social and Behavioral Sciences, 145, pp.97–102.

Bhasin, M.L. (2015b). Creative Accounting Practices in the Indian Corporate Sector: An Empirical Study, International Journal of Management Science and Business Research, 4(10), October, 35-52.

Bhasin, M.L. (2016). Combating bank frauds by integration of technology: Experience of a developing country, British Journal of Research,3(3), 64-92.

Bhasin, M.L. (2016). Fraud Scenario Prevalent in the Banking Sector: Experience of a Developing Country. The East Asian Journal of Business Management, 4(4), pp.8–20.

COSO (1992). Internal Control-Integrated Framework. New Jersey: COSO.Retrieved August 6, 2014, from BBC:

Cressey, C. and Martin, P. (2002). The Handbook of Fraud Deterrence.

Cressey, D.R. (1953). Other People's Money. Montclair, NJ: Patterson Smith, pp.1300

Clinard, M.B. and Cressey, D.R. (1954). Other People's Money: A Study in the Social Psychology of Embezzlement. American Sociological Review, 19(3), p.362.

Dewar, R. 2014. 'The Triptych of Cyber Security: A Classification of Active Cyber
Defense'. 6th International Conference on Cyber Security.

Dunn-Cavelty, M. (2010). Cyber Security in A. Collins, Contemporary Security Studies. Oxford: OUP

Gao, L. (2015). Long-Term Contracting: The Role of Private Information in Dynamic Supply Risk Management. Production and Operations Management, 24(10), pp.1570–1579.

Haynes, A. (2005). The effective articulation of risk-based compliance in banks. Journal of Banking Regulation, 6(2), pp.146–162.

Holtfreter, K. (2004). Fraud in US Organizations: An Examination of Control Mechanisms. Journal of Financial Crime.

Hooper, M. J, & Pornelli, C. M. (2010). Deterring and detecting financial fraud: A platform for action. http://www.thecaq.org/docs/reports-and-publications/deterring-and-detecting financial-reporting-fraud-a-platform-for-action.pdf? Retrieved on 2 August 2014.

ISO 31000 Risk Management. Available online: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/iso-31000-risk-management.html (accessed on 16 June 2019).

Scherer, M. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies and strategies. Harvard Journal of Law & Technology29 (2): 353–400.

Scherer, M.U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. SSRN Electronic Journal.

S. Velampalli, W. Eberle. (2017). Novel graph based anomaly detection using background knowledge Proceedings of FLAIRS 2017, AAAI Press pp. 538-543

Swain, S. & Pani, L. K. (2016). Frauds in Indian banking: Aspects, reasons, trend-Analysis and suggestive measures, International Journal of Business and Management Invention, 5(7), 1-9.

Appendix – Questionnaire

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

DEPARTMENT OF PROJECT MANAGEMENT

Topic of study: Evaluation of the role of NG|Screener Project implementation on fraud prevention: case of commercial bank of Ethiopia

Dear Respondent:

The purpose of this questionnaire is to 'Evaluate the role of NG|Screener Project on fraud prevention. This study is a partial fulfillment of a Master's Degree in Project Management at Addis Ababa University School of Commerce, College of Business and Economics. I hope you will give me your kindness in giving genuine and frank responses will contribute vastly to the quality of this study. Your responses are highly important only for this project research work and am confident that your responses will only be used for the intended research analysis purpose your response is highly appreciated.

I would like to express my heartfelt thanks in advance for taking your time to complete this questionnaire. In case, if you need any clarification about this research questionnaire please contact me:

Melese Gessese +251-920531603 natnaal@gmail.com

Thank you for your cooperation and Time.

SECTION A: Bio-graphic Data of Respondents

1. Sex 1) Female ☐ 2) Male ☐

2. Educational level:

1) Diploma ☐ 2) Degree ☐ 3) Masters and above ☐

3. In which age group are you?

1) 25 and below ☐ 2) 26-35 ☐ 3)36-45 ☐

4)46-55 ☐ 5) Above 56 ☐

4. Position held at CBE?

1) Manager ☐ 2) team Leader ☐ 3) Senior IT Auditor ☐

4) Senior Application Analyst ☐ 5) Customer Service Manager ☐

6) Application Analyst ☐

7) Other Officer ☐ Please specify……..

5. How long have you been working with commercial bank of Ethiopia?

1) Below 1 years ☐ 2) 1-5 years ☐ 3) 6-10years ☐

4)11-15 years ☐ 5) Above 15 years ☐

SECTION B: Questions related with the objectives – Role of NG|Screener Project implementation on internal fraud prevention.

Instruction: Please indicate the extent to which you either agree or disagree with the following statements by marking a tick mark √ in the appropriate column to the right side where rating scale as

Use scale 1= Strongly Disagree 2=Disagree 3=Neutral 4=Agree 5=Strongly Agree

1. To what extent do you tend to agree with the following items seek to determine the relevance of NG|Screener project implementation role on internal fraud risk prevention challenges among CBE core system areas?

NO	NG|Screener role on internal Fraud prevention challenges among CBE core systems	1	2	3	4	5
1	deletion Find out loophole identification and analysis on systems and applications					
2	Detect Forgeries and falsification of documents					
3	Identify Fraudulent money transfer and withdrawal					
4	Control Abuse of Administrator Privileges					
5	Identify Account and Customer-opening fraud (opening with fake identification)					
6	Mitigate Unauthorized Withdrawals					
7	Monitor and prevent Un authorized use of back end privileges					
8	Detect Transaction Reversal and					
9	Identify Four Eyes Violation on transactions					
10	Identify Theft of confidential information of customers					

2. To what degree do you tend to agree with the following statement relating to role of NG|Screener system implementation on fraud prevention impact in internal control improvement areas?

NO	Degree of NG|Screener role on fraud prevention improvement areas across the bank environments	1	2	3	4	5
1	Improve cyber security of the bank activity					
2	Great role on build strong management control and Provide continues input					
3	Increase internal audit performance					
4	Enhance the bank line of defense on internal control system					
5	Influence to prepare fraud Controls Policy and procedure					

3. NG|Screener and role of Investigation on Fraud Prevention in commercial bank of Ethiopia.

	NG|Screener investigation role of fraud risk	1	2	3	4	5
1	The system provides accurate and reliable fraud data for compliance and law court.					
2	The system captures a long period of data for investigation from back history.					

3	The system identifies the fraud risk in quality data with a minimum time frame.					
4	The system provides data for anti-corruption and the legal cause of fraud.					
5	Provides the capability of management staff to investigate cases at the starting point.					
6	The system has the capability to identify the root causes of internal fraud risk loopholes in the core systems areas.					

4. The following items seek to examine the role of NG|Screener Fraud Prevention effectiveness on core system areas based on Internal Control System components in commercial bank of Ethiopia.

NO	1. Control Environment	1	2	3	4	5
1	NG|Screener is powerfully internal control of servers, applications and database environment					
2	The bank establish NG|Screener fraud risk prevention, detection and mitigation policies and procedure in the control environment					
3	NG|Screener fraud risk prevention and mitigation internal control systems decrease the frauds in the bank internal environment					
4	Are management overrides of established controls appropriately documented and explained and are deviations from such controls investigated by NG|Screener?					
5	Is NG|Screener in CBE has a very sound control environment to safeguard systems against abuse?					
6	NG|Screener system are control process, branch and district business and IT accomplishments on core systems environments.					
	2. Risk assessment	1	2	3	4	5
1	The role of system has an appropriate strategy of identifying the bank fraud risks internal control risk assessment.					
2	The control system/technology is able to identify the location and the performers to assess the fraud risk related activities					
3	NG|Screener provide bank risk valuation based on violation risk conditions using activities.					
4	NG|Screener periodically identifies internal factors which could cause financial and IT systems fraud (Risk identification).					
5	NG|Screener in CBE report risk issues when they appear and treat them comprehensively (Risk response).					

6	The system is powerful to assess risk causes and the likelihood of the risk occurrence (Risk evaluation).					
	3. Control activities	1	2	3	4	5
1	NG|Screener internal control system can detect and mitigate every areas of fraud risk and other illegal activities.					
2	The system identify the errors that leads to misrepresentations in the financial reports.					
3	The system captures all core system operational and IT activities for controlling each occasion of activities Control.					
4	NG|Screener system in the bank has control over its employee activity and records					
5	System Management control activities consider all the relevant core systems business processes, information technology and locations where control activities are needed.					
6	The system contributes to management selects and develops control activities that are designed and implemented to restrict technology access rights, alert identified fraud risk to authorized users to protect.					
	4. Information & communication	1	2	3	4	5
1	NG|Screener provide collected Control information‘s data are communicated to the management staffs.					
2	The system collected Transactions and employee data activities and classified to provide reliable information.					
3	The system share to illegal activities control reports to the accountable organ to handle the concerns in fraud.					
4	NG|Screener produce reports that contain operational, financial, customer and non-financial and compliance-related information about core system operations					
5	The system has effective automatic reporting processes in communicating to all process, branch and district responsible authority in CBE.					
	5. Monitoring activities	1	2	3	4	5
1	NG|Screener monitors core system business and IT environments to achieve the bank objectives in fraud prevention and mitigation.					
2	NG|Screener monitoring dashboard could reduce the occurrence of fraud risk activities.					
3	System provides visualization dashboard of real time data and back history activity data to all management controls staffs.					

4	System in the bank provides data to reviews employee performance activity monitoring based on the assignee level.					
5	Internal audit identifies and make auditing activity using System data provides and periodically to ensure compliance					
6	Is NG|Screener fraud prevention tool is AI and machine learning monitoring behavioral and activity analysis?					

5. Please indicate the extent to which you either agree or disagree with the following system Fraud prevention statements

NG|Screener in fraud prevention		1	2	3	4	5
1	The bank able to establish fraud prevention policies					
2	System fraud prevention capability improve internal control system area exhaustive					
3	System is computerized fraud prevention methods					
4	The possibility of fraud occurrence is reduced by means of NG|Screener fraud prevention system.					

1. What do you benefit from the implementations of NG|Screener fraud prevention project implementation?

   _____

   _____

2. To what percentage do you agree the system/technology reduce fraud risk prevention in CBE?

   _____

   _____

3. Do you have recommendations for the bank fraud risk prevention in commercial bank of Ethiopia?

   _____

   _____

Thank You Again