APPROVAL FORM

The undersigned certify that they have supervised and recommended to Midlands State University for acceptance of the student, **R136968P** dissertation entitled:

'An assessment of the effectiveness of operational risk management practises at PSMI Westend Hospital.'

The dissertation was submitted in partial fulfilment of the requirements of the Bachelor of Commerce Honours (Degree) in Business Management.

…… **……**

SUPERVISOR **DATE**

…… **……..**

CHAIRPERSON **DATE**

…….. **……..**

EXTERNAL EXAMINER **DATE**

RELEASE FORM

NAME OF STUDENT	R136968P
DISSERTATION	'An assessment of the effectiveness of operational risk management practises at PSMI Westend Hospital.'
DEGREE PROGRAMME	Bachelor of Commerce Business Management Honours Degree
YEAR GRANTED	2017

Permission is hereby granted to Midlands State University Library to produce single copies of this dissertation and lend or to sell such copies for private, scholarly or scientific research only. The author reserves other publications rights and neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

ADDRESS 14 Van Praagh Ave. Milton Park, Harare.

CONTACT NUMBER 0774 202 439

SIGNED: …….. **DATE**.....

DEDICATIONS

To my, parents and my brothers may this be the benchmark for the least of your future achievements. And to everyone else who follows their dreams tirelessly.

ACKNOWLEDGEMENTS

"Plans are only good intentions until they immediately degenerate into hard work." Peter Drucker.

I thank Jehovah who has always shone a light in my path all the days of my life and in every one of my endeavours.

Much appreciation to the Midlands State University, Faculty of Commerce, Business Management Department for allowing me to carry out this research. I am indebted to my supervisor, who has shown me direction and support as well as motivated me to work to the best of my abilities during this research.

Special thanks to PSMI Westend management and staff for allowing me to carry out the research and actively participating in the research through responding to questionnaires and interviews that were instrumental to the success of the research.

Love and deepest appreciation goes to my parents, Mr and Mrs Mandeya my brothers Ngoni and Lyton Mandeya and all other relatives who have provided me with love and support throughout my academic life. I am also grateful to my colleagues Belinda Makwanda and Kudakwashe Machinyi whose support and insights helped in the completion of this research.

Abstract

The study was motivated by persistent operational risk exposures which could be pointed in daily operations at PSMI Westend Hospital and challenges have led to failed quality services and smooth running of operations in the organisation. The purpose of the study was to assess the effectiveness of operational risk practices at the organisation and to establish alternatives which can be used to mitigate and take control of the operational risk exposure the organisation is facing.

The research explored literature for enhancing an understanding on the categories, measures, factors and management strategies of operational risks. The study took descriptive research design. Data was collected using only self-administered questionnaire thus relying on the quantitative nature of research study. Data analysis was conducted by using Microsoft office suit to generate descriptive and inferential statistics.

The research findings of the study indicated that weak operational risk management strategies were being used to management the risk exposures which were affecting the organisation and its service provision as so many challenges were heighted in the study. Alternative strategies on management of risks which arose due to failed process, human error and disruptions of information systems which the organisation uses were also suggested in the study.

Based on the findings of the research it was concluded that the organisation should invest in technologies that assist in the detection and monitoring of operational risks, setting of capital reserves which are used to manage operational risks as when they occur and provide refresher courses to all staff such that management of operational risk cannot be a management issues only but rather every staff member's business.

List of Acronyms

PSMI-	**Premier services medical investments**
PSMAS –	**Premier services medical aid society**
PSP –	**premier services pharmaceuticals**
WEH –	**Westend hospital**
FML –	**First Mutual life**
FLIMAS –	**Fidelity life insurance medical aid society**
ORM-	**Operational risk management**

List of tables

List of figures

Table of Contents

Chapter One

1. Introduction

This chapter covers on section concerning background of study and statement of problem. It further highlights on the objectives of the study and research questions which are to be used to test relationships of variables to be discussed in detail in the study. Limitations and delimitations are also to be pointed out and encountering remedies to the challenges.

1.2 Background of study

The prevailing economic conditions which have been noted with companies scaling down, seize operations and some going under judicial management reflects economic performance faced by Zimbabwe. Constance Chamukure, 5 May 2016, reported that a figure totaling 81 companies had closed down their operations in the first quarter of 2016 and further expanded that, the number also rose to 229 companies in the second quarter of 2016 (Zimbabwe Independent, 1 July 2016) due to hardships facing the economy among including the worsening of the cash shortages in the economy, high cost of capital and capacity underutilization. Industries in which companies closed down includes, construction industry, clothing and also the retail sector.

Premier Services Medical Investment (PSMI) is a company that is trading in health system sector and it is a strategic business unit of Premier Services Medical Aid Society (PSMAS) which came into being under the blue ocean strategy of PSMAS to form an integrated medical insurance into medical services provision. (Muyambo, 2016). PSMI has become the leading medical health service provision institution in Zimbabwe and with its several units among hospitals, clinics, pharmacies and clinical laboratories situated across 10 provinces of Zimbabwe. PSMAS subscribers are the main patients with dominant percentage who seeks medical health care to PSMI units. PSMAS subscribers use their medical aid cards in PSMI units during the process of accessing their medical aid benefits. Patients claim forms are then completed and taken to PSMAS such that payment is then put through to the service provider in the amount of service provided to the patients. Hence there is a thin line that can be noted from PSMAS and PSMI to be said there are 2 different organisations that trades and runs operations separately.

PSMI as medical service provider also offer its service to other health insurance companies such as CIMAS, FLM, Flimas, Heritage life insurance and other medical aid societies. AS the As, measure to make an easy of payment, the PSMI medical units also take pocket payments for its services provisions and sale of medical drugs to patients. This form of payment has become very dominant due to the reason that closure of companies has left so many people with less to spare on payment of medical aid coverage but to resort to use of cash payments on medical services.

Table 1.1: PSMAS performance statistics for the year 2013-2015

Years	2013	2013 (%) Change	2014	2014 (%) Change	2015	2015 (%) change
Revenue	$220,348,551.00	100	$210,698,325.00	95.62	$204,322,758.00	92.73
Costs	$240,831,061.00	100	$265,965,715.00	110.44	$289,449,059.00	120.19
Profit / (Loss)	($20,482,465.00)	100	($55,267,390.00)	269.83	($85,126,274.00)	415.61

Source: PSMAS Financial Statements (2013 - 2015)

However, table 1 is showing PSMAS performance for 3 years. It can been noted that revenues continuously declined and operating cost skyrocketing resulting in the company making losses for 3 years in a row. As being shown in the table, in 2013 the organisation made a loss of $20,482,465 and the figure increased to $55,267,390 and to $85,126,274.00 in 201. Given such statistics the company is failing to meet its obligations which among is the payment of claims from the service provider, PSMI and also claims from other medical aid societies.

PSMI in 2016 decided to embark on business restructuring strategy as a measure to encounter several problems which were mushrooming on daily basis and as well as to equate the business operations with the prevailing trading environment. The problems in PSMI ranges from human resources issues, financial instability which then tend to fuel more problems and also operational failure issues.

The restructuring strategy did not bring much success on the table as expected by the directors. The strategy was meant to resolve the existing issues in the organisation but in actual essence started developing other problems which the directors had overlooked. The process involved

terminations of other employees` contracts leaving some huge gaps of tasks to be completed by those who were not sent home. Unpaid overtime and increased work overload and also delayed salary payments became common phenomenon in the organisation. Muyambo (2016) second the argument that there was delayed payment of salaries to Premier Services Pharmaceutical (PSP) which is a unit to PSMI. Starting from management were being owed 5 months and non-managerial employees were being owed 3 months constituting a figure totaling US$450,000.

Furthermore, maladministration and corruption has led to PSMI exposed in local papers for failing to pay salaries on time and also to honour its dues to creditors on time and at the same paying director salaries and allowances that constituted 45% of the wage bill. (Constance Chamukure, Zimbabwean Independent, 17 July 2015). Dropping trend in consumer confidence increasingly erodes the institution brand down and furthermore noted with termination of contracts by some specialized doctors form the organisation as their owing's from PSMI were not forthcoming. Various units of the organisation have been found with long queues of patients awaiting service provision.

Drug shortages has been noted in shelves of all PSMI units. Extension of debtors' payment period by the organisation has forced the organisation to trade on cash delivery with its suppliers. This has not only worsened relationships between the organisation and its trading partners but rather proven to be very expensive and accompanied by limited purchases on quantities of required supplies. As suppliers are now reluctant to offer credit facilities to the organisation due to unpaid balances owed, has led to drug shortages in pharmacies, clinics, hospitals and other units which operates with medical drugs. According to Constance Chimukure, The Zimbabwean Independent, 17 July 2015 further highlighted that management was failing to secure drugs at PSMI pharmacies.

However, debt management system in use has been noted with some weakness as evidenced by the table below.

Table 1.2: PSP Debtors figures for year 2012 - 2014

Year	Debtors' amounts ($)	Statistical changes (%)
2012	$462 409.67	-
2013	$536 009.80	13.73%
2014	$633 009.98	15.30%

Source*: Muyambo T, (2016) An investigation of the debt management practices on the performance of Premier Service Pharmaceuticals (PSP)*

According to Muyambo (2016), PSP as one of the units under PSMI organisation showed the struggles this unit was facing towards controlling of its debtors' ledger balances. As illustrated by the table below in 2013 debtors' balances were $536,009.80 and the figure rose to $633,009.98 showing an increase from 13.73% to 15.30% of the money balances which were held outside. According to Carlos (2010) poor debt management structures can inhibit a company's ability to ensure financial stability by affecting operations and putting the company's balance sheet under much pressure. Furthermore, sound debt management strategies can be instrumental in ensuring financial stability, by creating a liability structure for the debt that sustains low level of refinancing risk.

Revenue collections had not been forthcoming especially disbursement from the treasury which had allocated 120 million dollars for the year 2016, with which every month had been allocated a disbursement of 10 million dollars to the parent company PSMAS. Civil servants constitute the majority of the insurer's client base by a magnitude of 850 000 persons which are insured by the government. Eweje (2014) opined that contraction in revenue collections have noted to be the reason behind, failed operations and poor overall performance being cited in state owned enterprises. As such insignificant revenue collections from the government to PSMAS posed a challenge to the insurance company to channel significant balances for the services rendered to PSMI. Difficulties in smooth running of operations have been noted in all PSMI units including Westend Hospital.

The information technology systems which are in use in PSMI has dilapidated and become very obsolete to such an extent that at most cases the system can boot out users, giving wrong readings of the actual physical drugs stocks hence huge variances are noted every time without

proper measures taken from those noted variances. Drug embezzlement cannot be acted upon if the reliance on the system has got some biases.

Moreso, due to high cost of operations that were being experienced by PSMI this has become challenging for some units such as hospitals to afford cleaning chemicals which are needed most in cleaning theatre rooms and patient rooms among other vicinities in which hygiene has to be exercised as first priority. According to Zimmarman (2011) high cost of production in companies produces three elements which are far more significant than profit reduction and these include; operational efficiency, reduce commitment and unnecessary cost reduce profit, cash flows and the availability of resources. This has been noted at Westend Hospital where the challenge of high operational costs which is affecting PSMI has posed challenges to the diet of patients as repetition on meals has become more frequent.

The state of meals in PSMI Hospitals no longer conform to the diet requirements for patients as the portion per patient continuously decrease in size due to the shrinkage in financial resources of the organisation. This has affected the welfare of patients as the regulations of the hospital does not allow patients to bring in cooked food during their time of stay.

Failure to come up with sound financial strategies has been noted in the institution as there is consistent delay on financial reporting by other units in the organisation. According to Warren et al (2012) inferior information or inaccurate information can have devastating effects on plans. Some units in the organisation delay with approximately close to two months to produce financial results and as such financial strategizes which are formulated are based on unreliable information. However, the organisation in most times is failing to manage all the costs centres and ends up resorting to use of cash revenue collections to service mushrooming problems as and when they occur.

1.3 Statement of problem

Close attention on macroeconomic conditions have made companies to focus on operational efficiencies against goals on profit maximization, improved performance or rather trade break evenly. But how much risk should companies take to achieve the ultimate goals? PSMI Westend Hospital is faced with risk exposures which are coming from its day to day operations. The study

seeks to provide strategies which can be used to counter such risks as they are cause serious damage to the intuition on both monetary and non-monetary effect.

1.4 Research objectives

- To identify strategies that are used to manage operational risk at PSMI - WEH
- To evaluate the effectiveness of strategies that are used to manage operational risks at PSMI - WEH
- To determine challenges that are faced in managing operational risk in PSMI
- To establish the effects of operational risk management in PSM - WEH
- To establish alternative strategies to manage operational risks at PSMI - WEH

1.5 Research questions

- Does PSMI have proper systems in place to manage operational risks?
- Can PSMI effectively manage operational risks?
- To what extend is PSMI exposed to operational risks?
- What are the implications of operational risk management in PSMI – WEH?
- What are the specific recommendations for management of operational risk management at PSMI- WEH?

1.6 Significance of study

1.6.1 To the researcher

As a regulatory measure, this study is going to help the researcher to fulfil part of the requirement of the Honours Degree in Business Management, at Midlands State University

1.6.2 To Premier Services Medical Investment

Research is meant to assist the board and management of PSMI to formulate and implement the results produced by this research towards management of operational risks in work place as this has got much impact to the success of the business.

1.6.3 Theoretical

The theoretical perspective of this research centres on constructive matter as a means to cover up the gap that has been noted by the researcher and to further add on the current body of knowledge.

According to Abkowitz (2008) operational risk management has been described as the proactive measures that are put in place for major disasters as a means to mitigate or eliminate losses brought through exposure. HSE (2008) further claims that operational risk management and quality are key components in the provision of services to customers.

The topic of operational risk management is an area of study that has been on spotlight being evidenced by researches authored Sewanyana (2006) on operational risk management, organisational environment and organisational performance at Stanbic bank Uganda Limited, Afambo (2006) on operational risk capital provision for banks and insurance companies and also a study carried by Martin at el (2013) on, Operational risk management: Practical implications for the Southern African Insurance Industry. But it can be argued that wide researches on the subject matter has been more centralized on commerce and less attention has been given to institutions in the healthcare system. If this is not addressed the problem of operational risk will worsen.

1.6.4 Practical

The purpose of this research seeks to achieve an understanding on how operational risks can be managed in an organisation which is serving in healthcare system. Focus is going to be centred on tools, techniques and strategies which can be implemented to ensure that operational risk in organisational processes are mitigated or even eliminated.

It further seeks to provide alternative strategies which can be used to manage such risks on both private and public organisations which provide healthcare, such as Westend Hospital and Parirenyatwa respectively.

It is going to also add on the current board of knowledge and concentrate on the gap identified by the researcher. The research on operational risk management is widely researched on financial institutions and yet the health sector is also affected by the same operational risk variables.

The research is going to give an in-depth analysis understanding on the effects of operational risks to the company and also companies serving in healthcare system and other entities in various industries

1.7 Delimitations

The study is going to focus on PSMI – West End Hospital under the assumption that problems affecting healthcare service providers, that is form both private and public sector can be depicted from this particular institution.

The study is to focus on period that is from 2014 – 2016 for which the student has access to information.

1.8 Limitations

- The research was carried out at Westend hospital one of the units of PSMI with the assumption that situations which are affecting the unit are the same situations affecting all units located in different locations in the country
- The research study was conducted purely on quantitative data collection method. Integrating additional methods of data collection could have increased the scope of the study and the depth of analysis.

1.9 Assumptions

- If PSMI effectively manage operational risks, it can successfully attain profit

maximization and performance.

- Required information on PSMI position to give current status of the organisation will be obtainable.
- The findings of the study can be generalized to all institutions in the healthcare system.

1.10 Chapter Summary

PSMI as any organisation in the service provision medical services is experiencing challenges in keeping up with the required standard service provision to its stakeholders. The stated problems which have been identified in the chapter has triggered an interest in the researcher's drive to conduct a research on effectiveness of operational risk management practices at Westend Hospital and to establish strategies which can be used to mitigate or eliminate the risks.

Chapter 2

Literature review

2.0 Introduction

The chapter relates to literature review on operational risk management and focuses on the theoretical and empirical evidence which has been drawn from various sources denoting researches which have been carried by various researchers for the past decades in various industries across the circles of commerce.

2.1 Overview of risk and the general theory of operational risk

Several definitions of risk have been put forward by various scholars and its trend usually narrowing down to negative implications. Risk, theoretically and in practical world, has been seen as the adverse of desired results hence various fields in the scope of entities and organisation has put several mitigating measures towards the subject of interest. Guttge and Lee (2011) legally, risk has been defined as the product of, the extend of the expected damage and probability of its occurrence. Potential harm that may be due from some present process or future event may be perceived as risk for example decisions which are put forward as future strategic plans for companies, negative motion which makes the achievement of the targets impractical (Flammini, 2012). Losses for unforeseen events can also fall in the definition of risk.

According to Horcher (2005) risk and exposure has been defined separately, coming up with two elements; probability of loss while the second one exposure, being the possibility of loss and as such risk arise as a result of exposure. Andersen et al (2014) argued that risk can be internally driven by factors that will be in the organisation and so are the external variables, can also influence the extent to which an organisation can be exposed to some risks. Risk which are internally driven include, malfunction of internal processes and reluctance of management whilst

external risks variables comes from the environment in which the organisation is particularly trading in.

The variables in the environment include changes in marketing mix and demand of the products/services of the organisation and changes in ways in competition management is taken by other firms in industry, socio-economic platform and the political environment. Overly the dimension of risk has great impact to the reputation, legacy and continuity of the business.

Figure 2.1, below shows the two broad categories of operational risk as argued by Groupy, Galai and Mark, (2001) in Koomson (2011).

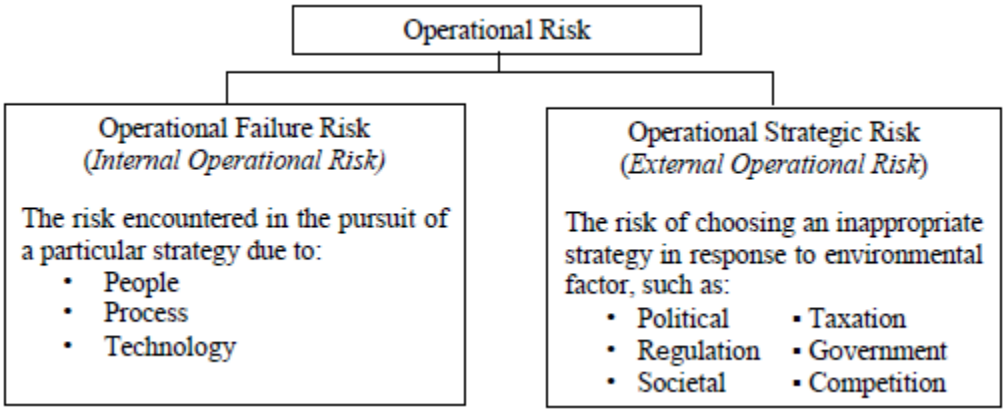


Figure: 2.1: *Two broad categories of Operational Risk (Koomson, 2011)*

The diagram is showing that operational risk is broadly categorised into two types, that is; operational failure risk which is risk that is driven by internal failure in processes, people and technology as result of trying to achieve an internal strategy. The second category is externally driven and it is called operational strategic risk. It arises as a result of choosing inappropriate strategies in response to environmental variables such as political, regulation, taxation, government interferences, competition and the societal factors.

In history of operational risk, events which dragged attention to the subject matter relating to huge losses have been noted in various organisations and in various industries. A call for attention towards management and devising of measures were put forward attentively by financial institutions. The table below is showing some of the cases of operational risk events.

It is important to acknowledge that risk is divisible in various categories such as strategic risk, financial risk, legal and regulatory, reputational, political environment, operational risk among other various forms (Heriot Watt University ,2011). Storkey (2011) defined risks in three categories as financial, business and operational and the standards for insurance companies. Whilst FS Prudential sourcebook for investment banks (2013) grouped risk in six categories along with operational risk, credit, market, group, insurance and liquidity forms the basket of risks category.

Risk of any nature coming from the denoted categories has negative effects towards the attainment of organisational goals like increased productivity, performance, market share and profit maximization. The risk which the researcher implies in the study relates to the operational activities that tend to be carried out in the daily operations in the hospitals operating in medical healthcare system in Zimbabwe.

2.1.2 Categories of operational risk in health care

2.1.2.1 Financial risk

According to Baker et al (2011), financial risk refers to the ability of any organisation to manage its debt and financial leverage while risk refers to the company's ability to generate sufficient revenues to cover its operating expenses. Financial management focuses on controlling mechanisms which are put in place to take control and absorb negative impact to the shareholders' investments and also the earning power of assets of the company. Financial risk management ensures that stakeholder interest apart from investors such as suppliers, employees and management are secured as well. Beside the argument of protecting investor, invested wealth financial management provides an argument that for the investors to earn more returns from their investment they have to invest in projects with high financial risks (Baker at et, 2011).

The process of financial risk management does not only relate to the avoidance of risks but involves the process of identification of potential risks and devising of policies and instruments to manage and also to monitor the risk before their impact to the organisation. According to Masenene (2015) the extent to which any organisation is exposed to financial risk lies more on the hands of the board of directors and the decision they make towards risk management based

on the available information in relation to the financial markets. Strategies which are made by board of directors have to be consistent with the internal motives and policies of the organisation. Financial risk is a broad area which includes mainly credit, liquidity and market risks.

2.1.2.2 Credit risk

According to Bun and Bradstreet (2007) a credit asset is a bundle of risks and returns and credit assets are in the form of loan, instalment credit, financial lease contract and accounts receivables. Credit risk or counterparty risk is defined as the potential default of a borrower or other party to a contract to honour his side of the deal on time and this could mean failure to provide promised loan facilitates or failure to pay debts within stipulated times to the contract as a result of changes in values associated with unexpected changes (Christoffersen, 2012). According to Lam (2014) the goal of credit risk management is to minimise company exposure to this form of risk by implementing policies and procedures which are used to select individuals or entities which should successfully qualify to this credit facility.

Healthcare system is an industry that specializes in service provision, hence more patients are admitted in to hospitals based on their health conditions and most of the time certainty on when they will be discharged is unknown. As such most hospital bills accumulate and according to hospital regulations, patients are not supposed to be detained for failing to pay their dues at time of discharge. As evidenced by literature nonbank financials and nonfinancial corporations struggle to put measures to eliminate risk as this is not part of their core business, however many corporations often are forced to take credit risk exposure that they would rather be without due to the nature of their operating environment which tend to be influenced by various factors, largely external. Bank for international settlements (BIS)(2000) advises on the formulation of strategies to mitigate such credit risk exposures so as to avoid other risks which are operationally related.

2.1.2.3 Liquidity risk

Christoffersen (2012) defined liquidity risk as conducting transactions in markets with low liquidity, which will be evidenced in low trading volumes and large bid ask spreads. As a result, an attempt to sell the assets will push prices low resulting in assets attracting low prices against

their fair value on the market or taking long before they are sold (Christoffersen, 2012). Duffie and Singleton, (2012) add that liquidity risk is risk which will arise as a result of adjustments in financial positions thereby increasing substantially the financial loss of the organisation.

As evidenced by literature the definition of liquidity risk, is risk which may cause companies or banks failing to meet short term financial demands, and the risk arose due to the failure of the company to convert securities of hard assets to cash without a loss of capital and or income in the process. Liquidity risk focuses on the probability of loss arising from a situation where there will not be enough cash and or cash equivalents to meet the needs of depositors and borrowers or the sale of illiquid assets will yield less than their fair value or another instance can follow in the illiquid of assets failing to sale at the desired time due to lack of demand or buyers thus the risk of liquidity of the firm exposure arose.

Generally, such risk to firms relates to the financial performance of the firm and its ability to convert its debtors and inventory on time for the organisation to meet its daily cash demands or daily costs related operations of the entity.

2.1.2.4 Market Risk

According Bun and Bradstreet (2007) market risk is defined as the risk of losses an investment may face due to fluctuations in the market variables. There are various forms of market risk which include customers and products, product research and development and sales and customer services. Masenene (2015) highlighted that market risk which is also known as systematic risk cannot be eliminated as it is a variable that is driven externally but it is risk which can be hedged against. Market risk is risk which can overly affect the performance of the organisation.

Freser and Simkins (2010), potential risks can also be found in the process of formulating strategic plans within the marketing section plan, that is from the target market an organisation will decide to serve and as well as promotional strategies an organisation will adopt will result in huge losses in amounts that will not be recovered. Market risk variables includes, several examples such equity risk which deals with changes in prices of shares on the stock exchange, commodity risk which are mainly associated with changes in the prices of commodities such as

metal or grains, interest rate risk, which is risk associated with changes in costs of capital which in turn have ripple effects on cost structure of companies and inflation risk among several others.

2.1.2.5 Operational risk.

Storkey (2011) defined operational risk as a range of threats from loss of key personnel, settlement failure, and compliance failure, to theft, systems failure and buildings damages. Koomson (2015) referred to operational risk as a daily and continuous process which can affect the organisation across the year as it is not a once off event. Dexter at el (2007), European Investment Fund (EIF), (2010) and Basel Committee on Banking supervision(2011) defined operational risk as the risk which arises due to failure in internal processes, people and systems or from external events and further stresses that the definition takes into account legal risk, compliance risk and reputational risk but excludes strategic risk as part of the operational risk package which seeks attention as it has got negative effects for the organisation's life span.

Risk is highlighted in various circles of business life; operational risk management has been noted with a red flag across all industries include institutions operation in the healthcare system. Dexter at el (2007), suggested assessing, monitoring and controlling as means of managing operational risk in banks, companies in the insurance sector and various entities. It will be wise to manage operational risk in all forms it tends to emerge from as it has ripple effects towards the overall performance of the organisation as the same other forms of risks which have gained popularity over the ages. According to Christoffersen (2012) operational risk should be completely eliminated as the exposure to it, does not give any significant returns to the entity and as such this form of risk is managed through use of self-insurance or third party-insurance.

According to Carroll (2011) risk managers in healthcare institutions are faced by the following classes of risks; such as finance, insurance, claims management, event and incident management, clinical research, psychological and human healthcare and emergency preparedness and such departments in each and every institution have different level of operational risk exposure. The most common and known risks that have of late affected effectiveness of organisations operating in the healthcare system relate to operational risks, being a category which constitute various classes of risks which have dragged much attention to the subject matter.

The healthcare systems are changing and new ways on provision of services to patients and clients are evolving. There have been so many modifications to the regulation of the healthcare systems and institutions in regard to how risk should be managed. More statutes and regulations are being put in place as a measure to manage risk which are coming from the changes in the management styles in these healthcare systems. Demands on healthcare from the general populace have brought with it several risks in all corners and complexity in the administrations of healthcare institutions.

2.1.3 Categories of operational risks

Categories of operational risks that come from activities which are undertaken by the organisation on daily basis should be established. Carroll (2003) categorised enterprise risk into four classes which include hazard, operational, financial and strategic and he further mention that in categories there are medical professional liabilities, property, directors and employee compensation which take most of the operational risks to the spotlight. Javier (2017) and Hull (2010) in their view further considers that operational risks should be categorised in seven categories which had been classified by the Basel Committee on Banking Supervision report of 2002 such that management of risks in the organisation will be made possible. The **seven** categories which were classified in the report include:

(i) **Internal fraud**, which has been described as premeditated misappropriation acts by individuals on property or circumvent regulations, the law and company policies. Examples of such acts include intentional misrepresentation or misreporting of positions, employee theft and insider trading on an employee's account.

(ii) **External fraud**: this has been described as conduct which involve a third party with an intention to defraud, misuse property and evading the law. Examples includes robbery, forgery and damaging resulting from cyber hiking on company security protocols

(iii) **Employment practices and workplace safety**: this category looks into the company's on working environment with safety regulation of the organisation. The acts on this category has been described as risks which arises from inconsistent with employment health or safety laws or agreements or which result in payments of personal injury claims. Examples which were given under this category include violation on employee health and safety rules and organized labour activities

(iv) **Clients, products and business practices**: this category focused on risk which comes as a result of negligence to act professionally in the conduct of business activities to clients and the use of inappropriate products. Examples which fall in this category are as follows –misuse of confidential customer information fiduciary breaches, improper trading activities on company accounts, money laundering and the sale of unauthorised products.

(v) **Damage to material assets**: this category of operational risk that the company has little or no control over and examples include damage of company property as a result of external events impacting the organisation such as terrorism, vandalism, earthquakes, fire and floods.

(vi) **Business disruption and system failure**: operational risk can be derived from disruption of business or systems failures and this consist of hardware and software failures, telecommunication problems and utility outage.

(vii) **Execution, delivery and process management**: this form of operational risk looked into issues concerning failure of transaction process and process management disputes with trade counterparties. Examples of this nature of operational risk includes, data entry errors, incomplete legal documentation, collateral management failures, unapproved access given to clients' accounts and vendor disputes.

2.2 Factors influencing operational risk management

Factors which influence increase in operational risks rely on both internal factors and external factors and these factors cause huge losses in various businesses, in different sectors. The first aspect that influences huge losses that can be made by the organisation is human capital and the contractor behaviour. Harrison (2013) reviewed that contractor behaviour can be a major source of operational risk, and this can be contributed by the use of untrained labour force in tackling technical tasks which require skilled or personnel with the expertise to deliver quality work. He stresses out that managing employees can be very difficult because human capital is subject to changes in moods, behaviour and personality and as such humans are different from machines which are set to perform certain tasks and left on automation to perform the task till complete without diverting from the core objective.

However, having confidence in the type of personnel which are taken to be part of the organisation is very important in determining their ability to adhere to the organisation's policies, strategies and as such this will also help the organisation in mitigating or maintaining a standard risk management approach.

Culture of an organisation has been put on the spot light by Harrison (2013), that it also plays a vital role in either managing or exposing the business operational risks. The culture of safety is supposed to apply not only to the members of the organisation but also to the stakeholders such as suppliers who are delivering goods to the site of the organisation, service providers and customers or clients who have got business dealing with the organisation. Furthermore, HKIB (2013) supports that culture play an important role in driving attitudes and perceptions towards operational risks and that organisations should be the breeding ground for right risk culture, through their ranks and across the whole organisation.

Poor communication channels and reporting which are poorly structured, contributes to the risk exposures which are faced by the organisation. Risks which have been encountered in or during periods of executing tasks and noted potential threats to the organisation should be reported and documented such that corrective measures are taken based on their frequency of occurrence. However, the organisation should build reporting structures which are flexible and clearly monitor the stipulated safety regulations and their weakness such that they are regularly reviewed and updated.

Overly operational risk can stem from so many variables which ranges from those that can be in control of the organisation to those that the entity will not be in control of. Literature have proven that technological dynamics, changes in governing laws of the land, changes in political field and adverse economic conditions total affects how the organisation will manage and avoid itself from operational risks (Terry and Mark 2001 and Jacqueline, 2002). However related literature on operational risks provided insights on how management will try to reduce risks in their operations through internal procedures such as risk assessments, internal control activities, monitoring, information and communication (Masenene, 2015).

2.3 Implications of operational risks.

Operational risk is a broad topic which several back several classifications of risks which affects business operation unexpectedly. Several models to manage these risks has been introduced since the topic gained attention that it is an area of importance as popular credit and market risks. However, it is difficult to identify or assess levels of operational risks because it is derived from so many sources.

To effectively use existing models to manage operational risks the process requires data collection and systems for a very long period of time. According to BIS (2002) the challenge of data collection and acquiring technical equipment and investment of time in the process has been associated with several firms failing to manage operational risks. The requirements are embedded in in the Basel II of 2002, which is a framework designed to manage operational risks in organisation through calculation of how much capital should be invested aside towards hedging a firm against operational risk exposures.

The impact of operational risk to the organisations are far from the quantifiable loss that can be noted from financial institutions. McKinsey and Company (2017) highlighted four deadly sins of the impact of operational risks and these include:

2.3.1 **Embezzlement** - is defined as internal fraud which appears to have a contradictory effect on corporate markets valuations, net gains around the date when the event is first revealed.

2.3.2 Loan fraud- this risk is caused by borrowers who fraudulently obtain credit to the firm and later default on payment.

2.3.3 Antitrust- these are risk which arises due to some negotiations which the firm engages itself with its clients or customers. Companies are noted to engage themselves in dealings which involves provision of certain products and services on fixed price basis and changes in market will result in the firm making huge losses.

2.3.4 Compliance- these are risks which arise due to fines for various forms of malpractices which generate losses even before they take effect. According to the article, it has been noted that market reactions after such fines can go as far as 5.5% loss on shareholder value.

2.4 Concepts of operational risk management

Dealing with multitude of internal and external risks in the organisation is one of the most challenging stages in running operations of the business on daily basis due to increased transaction volumes, globalization of the business environment and changes in technology which has brought about complexity and uncertainty to the general business setup and management. According to Javier (2017) after defining operational risk, it is wise to take the second step to management of operational risks. Risk appetite of any organisation has much influence on the decisions which are taken by the organisation in putting forward tools which are used to control and mitigate risks.

Carey (2001) stressed that risk management is when effective and efficient cost reduction techniques are met and in return incidents are reduced or eliminated. However, Dan and Bradstreet (2007) emphasised on the point that risk management is not meant to eliminate risk that affect the organisation but to ensure that risks are kept at predetermined level of acceptability. Both further highlighted approaches in which risks can be mitigated which include; risk avoidance, loss control, diversification, risk transfer, risk retention and risk sharing. BPRD (2014) defined operational risk management by involving managing human error and inadequacies' and making sure that risk awareness in the organisation has been brought up and everyone has participated in the management control process.

Furthermore Abkowitz (2009) put forward an agreement to operational risk management which involves an aspect of preparation and response for major disasters. In his study, he pointed various cases on operational risk losses like; $9 billion loss of Banco Nacional due to credit fraud, $1.7 billion and subsequent bankruptcy of orange country due to unauthorised trading activity and $750 million loss of Allied Irish Bank in 2002 (Hull, 2010). As such, much attention was given on operational risk management arising in financial entities and firms trading in the insurance industries.

2.4.1 Operational risk measurement models

Operational risk measure is of vital essence in ensuring true causes of operational risk in the organisation are understood. According to Javier (2017) there are two approaches to operational

risk measurement and these are; “top-down” or “bottom up” models. The top down models focus on measuring operational risk of the industry or organisation as a whole and the results from the models will defined the required buffer to be set aside against operational risk and the amount will be distributed to all units of the business. Whereas the bottom up model start to measure risks in departmental units then all risks across the entity is aggregated to give the company profile towards operational risk exposure.

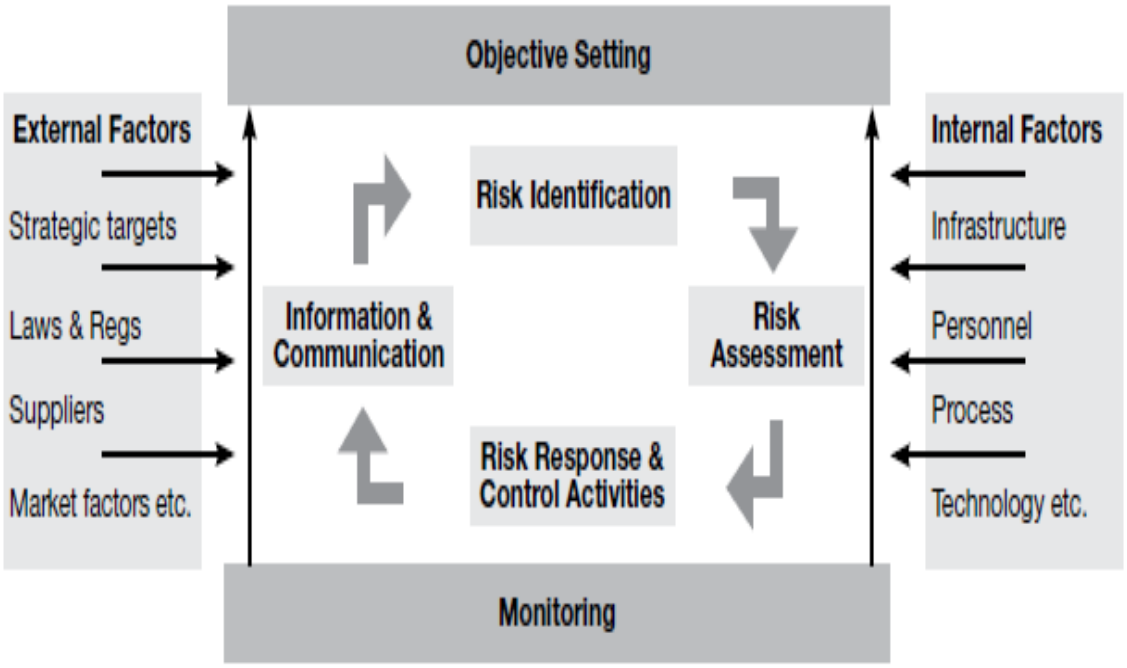
2.4.2 Operational risk management Model

Risk mitigation focuses on systematic reduction on extent of exposure to risk or the likelihood of its occurrence. Operational risks are different from other risks such as market, credit and liquidity as it is risk which appears during the course of business, more particularly on daily activities rather than risk which is associated with an exchange of an expected return. According to Lewis (2004) the emergency of operational risk has been noted with creating of statistical methods for measuring and monitoring of risks that relates to operational activities. As such operational risk management takes into account tools, techniques to effectively manage damages which are caused by their appearances in the day to day running of the business operations.

Basel committee on supervision of banks (2011) believes that forming a strong board of directors and senior management whose duties should be focused on building a culture that is guided by strong risk management should support and provide appropriate standards across the board. These standards include risk management issues and incentivising professionals and responsible behaviour which will help significantly on the risk reduction phase in the organisation. The principles which are set in the report states clearly that for risk mitigation to be achieved in the organisation strong control environment that utilises policies, process systems, appropriate internal controls and appropriate risk mitigation and or transfer strategies should be created and adopted by the whole organisation and its all functional areas.

Storkey (2011) drafted an operational risk management model which had an objective to be used in treasury department as a measure to mitigate operational risks which were activity based. The model showed that management of operational risk is a process which is similar to the processes which are taken in the general management of wide risk which affects business continuity and stability. This then poses a question that; What real risk management is? The answer relies on the

process of risk management which consist of identification, assessment, measurement, mitigation, monitoring and reporting of risks as denoted by the diagram below, the Operational risk management model.



Source: Storkey I - operational Risk Management Model

The risk management model reviewed that, to effectively manage operational risks risk managers should have an understanding of the forces which drives operational risk. As discusses in earlier discussion, that operational risks in an organisation are driven by two broad areas that is internal factors and external factors.

The model reviewed that internal forces which stimulate operational risks include infrastructure the company uses ranging from physical buildings to information systems hardware set ups, personnel which encompasses all the human errors and lack of skill which will result in false conduct there by exposing the company in to operational related risks. Furthermore, internal processes and procedural aspects which are followed by the organisation can also contribute to risk exposures which affect the company and lastly the technological advances and complexity

of the systems which are used by the organisation can expose the company into operational risks exposures if the information systems are too complex for employees to integrate with.

Whilst external forces which influence operational risk in the organisation include; **strategic targets** which are set by management as a means to achieve the overall goals can result in developments which will expose the company to risks which are operation-related as staff strive to execute the tasks, **changes in laws and regulations** either from industrial set up or policies which tend to be enforced by the government can also contribute to the operational risk which can affect the organisation. **Suppliers' relationship** with the company and the and changes in the markets factor are all part of the forces which business have little or no control over.
The forces from both end showed that various implications on failure to manage or take into consideration will affect company operations.

The management section of the operational risk management model
To effectively manage operational, risk the model highlighted four steps which are as follows:

(i) Risk identification.

According to BPRD (2014) and Storkey (2011) the first step firms should take in the management process of operational risk is through identification of risks that are in the daily processes and activities of the firm, products, services and systems. Tools which are used in the identification process of risks include among others, observation, actuarial models, scenario analysis, external data collection and comparative analysis in the procedural chain of entities. Risks identification covers frequency of occurrence which is typical damage and exceptional damage in order to quantify the rate of exposure the identified risk can bring to the entity. The exposure of risk to the entity is quantified in financial value of the losses expected to arise due to failure to manage the risks. The qualitative nature of the risk identified is primarily concerned with other losses which can be due to the occurrence of the risk. Qualitative nature of the risk focuses on the severity of the risk in question. Identification process as the first step in managing operational risk is followed by assessment process which is the second step in the model. It involves evaluating the severity of the damage expected in the event of occurrence of the misfortune.

(ii) Risk assessment

According to Hull (2010) risk assessment is an important component of risk management and its absence results in little hope of managing risks and achieving effectiveness in the organisation. HKIB (2013) states that it is important to quantify operational risk exposures by using results from risk assessment tools as inputs into models that estimates operational risks

According to Jorion (2007) risk assessment can be carried out using the following tools:

Critical risk assessment, this is where each department submits a subjective report on evaluation on sources of operational risk, as well their expected frequency and costs related

Key risk indicators, this where by a centralized unit develops a subjective risk forecasts through risk indicators, such as trading volume, number of mishandled transaction, staff turnover among other indicators

Formal quantification, this is where operational risk managers measure an objective distribution of operational risk losses from an event database

The process of risk assessment involves reporting loop holes in the operating systems of the organisation. Areas of focus when assessing centres on internal processes and other external variables which might have potential to contribute to the occurrence of the risk such as the changes in legislation, changes in the political and economic fields as well as the technological and societal changes. A precondition to risk assessment, objectives which are linked to different levels internally should be made. In the planning stage, management should agree on the types of categories to be used to define the nature of risks and their potential impact in the organisation.

The nature of risks which are faced by several administrations in the healthcare as evidenced by literature are picked on risk assessments, the issues which are brought to light relates; mandatory federal regulations, patient safety, existing future policies potential, medical errors, and legislation which impacts the field of healthcare

(iii) Control measures

Control measures form the last stage on the model of operational risk management. Actions which may be deem viable in mitigating or eliminating the risks exposure or damage of impact are considered. This stage majors on formulation of procedures and policies on how the identified risks in the organisation should be managed so as to ensure that overall goal of the

firm is achieved. The formulated policies should be communicated and implanted across all functions of the business. They should include all personnel of the organisation and should have involvement in auctioning the policy to ensure success.

Furthermore Hopkins (2017) argues that to effectively manage operational risks in an organisation formulation of policy which will focus on management of operational risks will be a larger risk management manual as the manual will provide guidelines and protocols to be followed in the management process. He adds that, there is type of documentation that is required depending with the complexity of the organisation to effectively built the risk manual and this documentation include; risk management administration records, risk responds and environment plan, event report and recommendation and lastly risk performance and monitoring reports.

(iv) Risk monitoring and reporting

Risk monitoring and reporting forms the third stage of operational risk management in the model created by Strokey (2011). This part of risk management focuses on the comparison of the actual risk levels with the desired or permissible levels on healthcare management guidelines or stipulated tolerance. Hopkins (2017) argued that an organisational manual or policy document on operational risk management should set out in detail systems and procedures to be used in monitoring performance as well as the means of reporting and communication on risk management.

The process also involves comparing risk management from another organisation with the one in which the organisation is using. This will give room to pick differences on areas in which the business is failing to manage. However, risk monitoring should be a continuous process in the organisation to ensure that acceptable range or levels of acceptability are maintained.

Adding on to the monitoring process, this is then followed by communication in the form of reporting. The reporting structure as highlighted in the model focuses on giving feedback whenever tolerable risk levels are noted to be departing from the acceptable levels to the responsible authorities such that remedial actions are taken to rectify the causes of such deviances.

2.5 Risk management strategies

Risk management strategies are focused on providing structures that will help in identifying, accessing and managing of risks through building processes which are used for updating and reviewing purposes. The assessments on strategies are developed based on actions taken. Coleman (2009) argued that management of risk goes through mechanical use of audits, checklist and actions that reduce risk.

According to Foster (2007) risk management strategies take into account the risk profile of the organisation, the risk assessment and evaluation of processes. Overly the risk management strategies can be derived from the operational risk model which was discussed above.

2.5.1 Strategies on operational risk management

An operational risk management strategy is defined as a plan for identifying, reducing and management of risk in a best possible way in relation to a trust' s service and business needs. In managing operational risk construction of strong internal control system should be on the centre of the whole process to ensure that anticipated or desired outcomes are achieved.

2.5.1.1 Use of internal control strategies to manage operational risks

Gelinas (2017) defined Internal control as a process that should be spearheaded by the board, management, and other personnel such that it will provide reasonable assurance regarding achievement of objective in the following areas like; effectiveness and efficiency of operations, reliability of reporting and compliance with application of laws and regulations. Internal control can be dived into two three broad elements which are preventive internal controls, detective internal controls and corrective controls (Turner, 2016).

According to Hall (2003) internal control activities are divisible in two broad categories which are physical controls and Information Technology controls. Physical controls strategies are meant to encounter operational risks which are caused by people. Physical controls consist of five classes of control activities which include; **segregation of duties, transaction authorization, access controls, supervision of accounting records, and independent verification** (Hall, 2003). Whereas IT controls consist of **input controls, processing controls**

and output controls.

2.5.2.1.1.1 Segregation of duties.

Hoffam (2002) segregation of duties and diversification are important part of operational risk management as it involves division of labour. Segregation of duties are especially important in work places where large values are concerned. According to Kondabagil (2007) segregation is one of the most fundamental internal control which is meant to encounter operational risk which can rise due to misconduct by personnel in the organisation. Application of this concept in the organisation begin by dividing administrative work from operational function to the operational system. In segregation of duties one individual should not be capable of initiating, authorizing, executing and subsequently review a transaction for appropriateness.

2.5.1.1.2 Internal communication

According to Kondabagil (2007), stated that internal communication is a key element in management of operational risks. Aspects of legal, reputational and operational among other risks can be managed and controlled if senior management communicates to key staff on how the provision of effective communication can be implemented in the company system. On the other hand, technical staff should effectively report back or give feedback to senior management on how systems are designed to work, as well as strength and weakness of the system. Kondabagil (2007) state that such procedures will reduce operational risks of poor systems design, including the incompatibility of different systems with the company, data integrity problems, and reputational risk associated with customer dissatisfaction when systems do not work as expected.

2.5.1.1.3 Access controls

Access control restrictions are technologies which hold details of credential for accessing a particular field within a database (Reuvid, 2010). Examples of control access credentials include; physical objects such as access badge, a piece of knowledge such as PIN codes, or a facet of a person's physical being such as a fingerprint and in some cases a combination of the stated credentials. Adoption of access controls as a strategy to mitigate operational risks can result in

reduction of operational risks cases in the organisation despite the fact that this form of technologies to identify and monitor activities tend to be very expenses at times.

Additionally, according to Hall (2003) and Kondabagil (2007) both concurred that organisation can safely install electronic control systems which provide security in most sensitive areas of the business operations, use of security cameras and enforcing security clearance protocols such that access codes are required for individual to access either information or use of company sensitive information systems.

2.5.1.1.4 Refresher courses

Abkowitz (2008) refresher courses are training sessions which are conducted with a goal to upgrade skills and knowledge of an individual. According to Tarantino (2010) training courses on operational risks can improve how employees in an organisation understand the need of managing risks and the effects of their decisions and actions towards stimulation of operational risk. Furthermore, Soprano et al (2009) added that training courses had to be designed to meet different types of requirements; providing introduction to the operational risk concept to all staff. Training sessions are supposed to be conducted periodical such developments in and new ways to handle issues are also reviewed and highlighted such affective execution of targets and objective of the company are achieved.

2.5.1.1.5 Preventive internal control

Hall (2003) assert that preventive control is the first line of defence in the control structure of an organisation and as such, preventive controls are passive techniques designed to reduce the frequency of occurrence of undesirable events. The objective of preventive control system is to ensure that the firm is guide against risk before they happen and these include fraud and errors that can as well result in misstatement of financial statements.

2.5.2 Use of Investigative internal control strategies to manage operational risks.

Investigative internal control focuses on provision of an insight on the cause of a particular risk. According to Turner (2016), investigative control must be included in the internal control system

as it provides help to employees to expose or discover errors, fraud or unauthorised events. Investigative internal controls tools include; physical count of inventory against records, reconciling bank statements to company books and as well as matching invoice orders prior to payments.

King (2011) suggested that conducting spot checks on undefined periods on high valued items and min-audits are part of the detective internal control. Such actives are carried out to mitigate or eliminate cases of fraud or false representation of statements to facts. Potential risks can be identified in the process and addressed such that their occurrence is avoided in the future.

2.5.3 Audits conducts to manage operational risks

Auditing is broad and it can be classified into two categories which are internal external auditing functions. According to Hall (2003) internal auditing is an independent appraisal function which is established in the organisation to examine and evaluate its activities. Internal audit function can be used to mitigate operational risk through carrying out of exercises such financial audits, performing IT audits to investigative an operation's compliance with the company's policies and legal obligation and evaluating operational efficiencies as well as dictating and pursuing fraud within the firm.

Whereas, **external auditing** involves use of third part professional in the evaluation and examining process of the organisation's process and records. External audits are more similar to those that are carried on daily basis with the organisation's internal audit committee but the difference lies in the independent opinion which is given by these third parties. External auditors, do not have material relationship with the organisation and as such their opinions are regarded to be free from biases and are less compromised (Hall, 2003).

Fraud audit is another function of the auditing community as its objective centres on the monitoring and setting of policies and processes that ensure that fraudulent activities are minimized as they are costly to the organisation. This form of audit got popularity in corporate governance and it has been regarded as a tool to be used in the internal control systems of the organisation. Hall (2003) state that sole objective of fraud audit is to carry an investigation on anomalies and gather evidence of fraud that may lead to legal conviction. Hall (2003) add that fraud audits are also used by organisations in investigating its own executives if there are

suspects on misuse of financial and non-financial assets of the business.

2.5.4 Developing of Human resources policy

People management strategy can be used as measure to reduce operational risks which are derived from human errors. According to BSTDB (n.d.) argued that to minimize risks which are due to human error companies should invest in control systems which advocate for development of a culture, in which employees will be aware of the operational risks. Furthermore, sources of operational risks from people can be derived from overworked workforce and this will result in significant processing errors

2.5.5 Risk and control culture

According to Tattam (2011) risk and control culture is a vital tool in the management process of operational risks in the organisation. Hence the author argued that since individuals have different cultures and norms so should be the organisation if it is to manage operational risk successful. A written document which defines behaviour of individuals which should be accepted in the organisation has to be developed, such that principled individuals are selected on the basis of their ability to observe the importance of operational risk and how they should be managed.

To effectively manage operational risks thorough the creation of risk controlled environment, staff should be trained and encouraged to suggest control and procedural improvements and such suggestions will also encourage creative thinking and ownership (Tattam, 2011). to individuals who would have contributed to that particular decision. In addition, incentivising individuals on their excellent participation in the management process has been argued to be crucial for a success operational risk management process.

2.5.6 Use of scorecard to manage operational risks

Use of scorecard in operational risk management involves an overall purpose of quantifying the results to come up with the extent of damage that can be brought by the occurrence of that type of risk. According to Hull (2010), operational risk managers should identify key determinants of each type of risk and then formulate questions for managers of business units to enable risk levels to be quantified. Scores are assigned to each answer and the total score for a particular risk

in an organisation can be used a basis for allocating operational risk capital. Scorecard in operational risk management is based on self-assessment approach which is also based on the experience and opinions of experts in the organisation who usually correspond to a particular business unit, (Giudici, n.d.). According to Javier (2017) states that assessing the extent of exposure of an organisation is subject to expected loss frequency, and the loss severity and the description of how to control the risk. The self-assessment is carried out periodically through use of questionnaires which are submitted to risk managers and these questionnaires give information on quality of internal and external control system of the organisation and these questionnaires provides information on frequency of some risks.

2.5.7 Use of physical asset management policy

According to Darling (2011) physical asset management strategy is a centralized and cross-disciplinary view to asset management which focuses on long term plans on how to manage asset to gain full optimization of the asset. To achieve this the author argued that an organisation should formulate asset management policy that focus on the specific mandate of principles, commitment, obligation and control framework for the development and implementation of the assets management strategy and plans.

In addition, Hastings (2015), asserts that asset management strategy provides resources and expertise to support the identification of potential risks and how they interact with business strategy. Asset management take in to account hazard analysis through identification of a series of potential risk and their significance before considering ways to overcome. The analysis process is conduct through use of risk register which is used to record all risks that have been encountered during use of the asset. Asset controlling section focus on times when assets should be maintained and specific periods in which processes are reviewed in order to reduce disruptions and potential risks which comes with the failure to do so.

2.5.8 Identification of variable relationships

Risk managers in organisations should establish relationships between variables in the organisation before taking decision on how to act on operational risks affecting the organisation (Hopkin, 2017 and Hull, 2010). Javier (2017) stated that causal relationships are described as losses that occur as a result of a cascaded of different causes and the causes and effects are

related by conditional probabilities. He was of the view that the loss distribution is simulated by taking into consideration of different relationship of variables and with the help of measurement models against operational risk this will provide an understanding of losses as they depend on determinants of operational risk.

Examples which can be given on assessments of operational risk relationships that exist between variables can be established in; the qualification of personnel hired in the organisation and mistakes arising from errors in the way transactions and services are conducted, and as well as two variables between the type of hardware and software the organisation is using against systems failure. If the cost is proven to be significant then a cost benefit analysis has to be conducted such that replacement of old machines and hiring highly qualified employees should be done to reduce the increase of operational risk exposure.

2.5.9 Allocation of operational risk budget

According to Hull (2010) states that business should allocate risk capital which will ensure smooth running of operational risk management activities in the organisation. He further stresses out that allocation of operational risk capital has effect of improving business units' return on capital. Managers should take note of the costs of reducing the risk, that it does not outweigh the benefits of reducing that particular risk. The overall result for allocation of operational capital and risk assessment should be that the business units or functions become aware and sensitive to the need for operational risk management. To achieves this successfully, the board involvement in the management process should be noted such that approval of risk management program and reviews are carried out on regular basis

2.5.10 Contingency plan and Business continuity management

Contingency plan is the formulation of an advance plan to be implemented on the occurrence of a specific future event (Andrew, 2010). Business continuity management has been regarded as the best practice in managing operational risks. A good plan which ensures continuity of an entity is the one which allows the business to carry its normal operations after occurrence of the unexpected. Edwin et al (2010) stated that business continuity plan has to become part of the organisation regardless of size or sector in which the business is operating in. To successfully achieve total commitment by every member in the management of operational risk in the

organisation, a culture of risk management should be embedded in the core values of the entity, and this will also boost shareholder confidence (Edwin et al, 2010). Elliott et al (2010) strongly supported that business continuity plan should be implemented in the organisation and to successfully achieve such a goal management should take note of two elements which are, firstly good communication system, rewards systems, and training for staff as well as control systems. The second element focuses on the clear organisational structure to be in place which is solid that cannot be shaken after occurrence of the unexpected.

2.5.11 Risk financing and operational risk management

Nonbank entities have several ways to deal with operational risk, as this risk is much worth to take as the returns are of little value to the organisation. Approaches to mitigate operational risks are in place and it is for the management to decide whether to take, eliminate or absorb the losses through its earnings. As earlier mentioned avoidance, elimination, termination and treat are some the approaches which can be used in managing operational risk in companies' daily operations. Other financing options towards management of operational risks which are available to them are:

According to Koller (2011) insurance has been widely used as a tool to manage operational risks as firms guard themselves through purchasing of products which are offered by these insurance entities. Tattam (2011) supported that products which are offered by these insurance service providers are meant to protect entities against financial losses and fraud on the part of any employee and damages of assets arising from operational activities which are carried out by the organisation on daily basis. Some of the products include directors' and officers' liability coverage which can protect against losses incurred by directors and officers alleged for wrong acts and by the firm for money it paid to directors to indemnify them for damages. Koller (2011) stressed out that insurance companies also offer life assurances for employee safety in the organisation, property, theft, fire and damages which can be caused by inclement weather.

2.6 Developing operational risk management environment

2.6.1 Developing effective operational risk management

In designing an effective operational risk management system, the Basel committee suggested seven principles and the King Report IV (2016) on corporate governance has also suggested the involvement of the board of directors in the process.

Developing an effective and appropriate risk management environment the board of director should be aware of the major aspects on the industry's operational risk and that it is an area which requires to be managed and it should be approved and reviewed periodically against the operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles for how operational risk is to be identified, assessed, monitored and controlled or mitigated.

According to Masenene (2015), the board of directors should ensure that the operational framework in her study toward banks and management of operational risks, that it should be subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff and the internal audit should not be responsible for operational risk management as the staff in that audit department are part of the operational activities of the firm.

Furthermore, senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be implemented across or the functional areas of the organisation and to every staff member of the organisation, and the involvement of every single member should be clearly understood and the responsibilities expected of each and every one. The framework implementers should ensure that the framework involvement in the organisation is also taking effect in the organisational products and services, processes and systems.

2.6.2 Effectiveness of internal process

The Basel II (2004), highlighted that control as a process, is effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objective in the following categories; effectiveness and efficiency of

operation, reliability of financial reporting, compliance with applicable laws and regulations. Internal controls are tools that facilitate managers with ways in which to effectively and efficiently avoiding serious problems such as overspending, operational failure and violation of laws. Internal controls form structure of policies, procedures which are put forward to provide reasonable assurance that management meets its obligation, objectives and fulfils its responsibilities

A system of strong internal controls can help to ensure that the goals and objectives of an organisation are met, and also that long term profitability targets and maintained reporting of reliable financial and managerial reports are given always. Javier (2017) suggested that operational risk can be reduced or even mitigated by firstly making use of internal control system of an organisation. To effectively achieve a sound internal control system the following must be considered; separation of duties, this has been described in sense of employees that those who are in charge of for example the commissioning of operations must not participate in trade settlements or accounting operations, dual inputs and reconciliations must be verified by two different sources and warning systems, warning systems, confirmations and amendment controls must be controlled by counterparty that can provide independent comparison and opinions towards some conducts.

The Basel (2001) provide the processes which are supposed to be followed when managing operational risks and the process has five components: risk assessment, internal control activities, information and communication and monitoring.

2.7 Chapter summary

This chapter focused on what other scholars have written in relation with the subject of operational risks. Strategies to manage risks which are derived from operations from operation have been attended to through viewing literature form books and journals. The next chapter looks into methods and tools which can be used to gather data so as to get a better understanding of the subject matter.

CHAPTER 3

Research methodology

3.0 Introduction

This chapter presents various data collection methods and analysis techniques used in gathering relevant data for this research. It describes target population and justification of sampling techniques used and furthermore, Primary (field) and Secondary (desk) information used in the research to address research objectives and research questions are to be given. Validity and reliability of the instruments concludes the course of this chapter.

3.1 Research design

According to Creswell (2013) research design is the type of enquiry within qualitative, quantitative and mixed methods approaches that provides specific direction for procedures in research study. Kothari (2004) defines research design as the arrangement of conditions for collection and analysis of data and further, expands that research design refers to the arrangements for collection and analysis of data in a manner that tries to combine relevance to the research purpose with economy in procedure so as to bring out best results. Thus, research design acts the blueprint of the research study in question and noting down procedures of data collection, the quality of data to be obtained with the help of selected research instruments and how data analysis is to be carried. The researcher adopted the descriptive research design for purposes of this study.

3.2 Descriptive research design

Descriptive research design is concerned with describing the characteristics of a particular individual or of a group (Kothari 2004). According to Knufer and McLellan (1994) argues that descriptive research design is primarily concerned with answering the What is question to the topic under investigation. Grimes and Schulz (2002) justifies that a good descriptive research must answer important questions, which are who, what, why, when, where and the sixth question

so what? Descriptive research design provides important element of reporting which is a clear, specific and measurable. The research design uses both qualitative and quantitative data to derive results after data analysis. The research design uses observational surveys and interview techniques to collect data about the topic in question and such data is then used for recommendations of specific strategies. Kothari (2004) argued that descriptive research design on sampling designs it focuses on use of probability sampling design (random sampling) and furthermore on statistical design a pre-planned designed for analysis must be used and well-structured instrument for collecting data should be designed for the purpose.

3.2.1 Justification of descriptive research design

The research adopted descriptive research design as this tries to bring out the current state of the environment by depicting a picture of the actual activities on the ground. Operational risks are affecting several institutions and not particularly those that are trading in financial markets or assurance services but rather across sectors including the healthcare system. The research design has got an ability to produce alternative strategies hence sort to be relevant in the study of operational risk management in healthcare system as the results are not solely going to help PSMI as an organisation. but rather both institutions in the healthcare system in the private and public sector.

According to Lodico *et al* (2006) highlighted that descriptive research design uses sample size of a large population, hence this has got more influence into the decision of the researcher in adopting this research design as he is dealing with a large population in PSMI organisation and generalizing of finds proves to be cost effective and also helps the researcher in covering more ground. The method adopted by the researcher has got an ability to produce large quantities of data due to its flexibility provided by the research instruments which are interviews, questionnaires and observation.

3.3 Target population

According to Greenland (2005), target population is defined as the population on which the researcher select participants who will provide the needed information related to the topic under discussion. Lavrakas (2008) add that target population is the entire set of units for which the

survey data are to be used to make inferences and further supported the generalization of sample findings to the entire population in study. As such target population refers to a group of individuals in a total population which the researcher is in interested in studying and the results derived from the sample represents the entire population since selected subjects to the topic in discussion are viewed to have common traits in nature.

Target population for this study was PSMI Westend Hospital, which was chosen by the researcher to represent the entire population of the PSMI organisation. Westend hospital is the largest unit in the organisation and as such, activities which are carried out in this unit are sufficient enough to represent other operational activities and information to be generalized across all units of the organisation.

The table below represents groups and departments at Westend Hospital and number of employees per each department.

Table 3.1: Target population

PSMI -Westend Hospital	Population	Sample size	Sample size%	Research design
Management	4	4	100	Questionnaire
Finance-Accounts	8	8	100	Questionnaire
Billing Department	10	7	70	Questionnaire
Front Desk Clerks	9	5	55.56	Questionnaire
Canteen	18	9	50	Questionnaire
House-keeping	24	8	33.33	Questionnaire
Pharmacy	10	3	30	Questionnaire
Nurses and Matrons	105	21	20	Questionnaire
Population Size	**184**	**65**		

The above table is showing target population, sample size and the research design which was used to collect data.

3.4 Sample size

Burmeister and Aitken (2012) defined research sample as the minimum number of participants required for qualitative investigation and answering of survey questions. Boyd (2014) adds that sample size is a subset of research samples from the target population and these individuals are deemed to be representative of the whole population. For the purposes of this research the researcher focused his efforts on management and departmental heads as these individuals have vast experience with the organisational processes and procedures as well as industrial knowledge due to their service in the medical and healthcare systems.

In coming up with the sample size for this research the researcher have adopted the following formula below from Yamane's formula (Israel, 1997);

$$n = \frac{N}{1 + N\ (e)^2}$$

n = sample size

N = research population

e = is the acceptable margin error

hence the workings towards finding the sample size for the research is as follows;

$$n = \frac{184}{1 + 184\ (0.10)^2}$$

$$n = 64{,}79$$

Therefore, the research sample size is equal to 65 as derived from the formula.

Of the 185, total number of employee's at Westend Hospital the researcher had to work with departmental heads, management and team leaders and a limited number of employees who were

selected based on their qualifications and availability. The researcher selected 65 respondents from the company. These individuals included were 4 from the management, 8 from the finance department, 7 from the billing department, 5 front desk clerks, 9 from the catering department, 3 from the hospital main pharmacy, 8 and 21 from the housekeeping department and nurses in wards sections respectively.

3.5 Sampling

Oppong (2013) defined sampling as the process of selecting subjects to take part in research investigation on the ground that they provide information relevant to the research study According to Jackson (2012) stated that sampling can best be described as a process which is used in statistical analysis in which a predetermined number of observations are taken from a large population. Much emphasis has been given on research subjects being selected for the purpose of giving relevant information to the investigation of the problem under discussion by the researcher

3.5.1 Sampling techniques

For the purpose of the research the researcher relied on convenience sampling, stratified sampling and judgmental sampling.

5.3.1.1Convenience sampling

According to Etikan (2016) convenience sampling technique is also known as haphazard or accidental sampling and it is a non-random sampling method with which members of the target population that meet a certain criterion such as easy accessibility, geographical proximity and availability at any given time are selected to the sample.

Justification of convenience sampling

Convenience sampling method was adopted by the researcher as this suit the working conditions of the organisation which under investigation. A group of 24 nurses and 8 individuals from the catering department who participated in the research were selected based on their availability and willingness to participate. This did not save time but also reduced biases on the information provided by subjects as they had voluntarily offered their time to fill in the questionnaires.

5.3.1.2 Stratified sampling

According Westfall (2008) to stratified random sampling is a statistical method that is used when representing a subgroup of a population which need to be represented in a sample and the subgroups are divided into strata based on their mutually exclusive criteria. Silverstone and Thornhill (2009) also add that stratified random sampling involves distributing the total population into different strata with similar characteristics and later take samples from the different strata. Generally stratified sampling involves division of the population in to subgroups of homogenous values and elements and later performs a random sampling or systematic sampling procedure when selecting subjects to ensure that each stratum is adequately represented

The researcher grouped in employees at Westend Hospital into Departments, defining their area of occupation at work places thus strata. The employees, based on their availability and volunteering to participate in the research exercise were given the questionnaire to provide their opinion on questions which were asked by the researcher. These respondents were selected from different departments (strata). The departments included were finance or Accounts, Billing, management, front office clerks, catering, Housekeeping, wards nurses, Pharmacy.

Justification of stratified sampling

This technique was relied on as it facilitates high chances of representation of the stratum or the population thus providing accurate information which can be generalized for that particular stratum.

5.3.1.3 Judgmental sampling

Judgmental sampling as defined by Oppong (2013), it is a method of sampling in which a researcher select research subjects who have knowledge of the issue/s being addressed by the researcher. Saunders et al (2010), judgmental sampling involves researchers using their own personal judgements in selecting participants best suited to address research questions.

Generally, judgmental sampling is a non-probability sampling method which can be used to select research subjects based on the researcher's knowledge and experience of the required

subjects to provide information as such it is based on the ability of the researcher in identifying research subjects which are relevant

Justification of judgmental sampling

The researcher adopted this sampling technique basis on the argument of expertise and working experience of subjects to the working environment. The researcher picked persons who had served the organisation for longer period and deemed to have important information to the research study and these subjects are deemed to have better knowledge of the institution. The 4 managers who had gone up the ranks and 6 departmental heads from the given departments who had been promoted to be team leaders in the organisation are among the subjects who were selected to provide answers to the questionnaire provided by the researcher.

3.4 Sources of data

According Abawi (2013), data is information that has been gathered in a research study by a researcher yet to be analysed so that it will be transformed to meaningful information. Source of data can be divided into 2 categories that is **primary and secondary data**. Data can be qualitative or quantitative based on the purpose of study and the environment in which the data is being collected.

3.4.1 Primary data

Generally primary data is information which has been obtained from respondents as first-hand information. According to Currie (2005) primary data is gathered when required information needed is not found in published sources thus secondary data. When collecting primary data, there are 3 widely methods which are used, which are survey, interviews and observational method. Qualitative data largely falls in to primary data as this is information that is obtained from research respondents through use of various data collection tools.

Qualitative data is information which is provided by a research subject being interviewed and the information is said to be subjective because the information is a product of the respondent's personal opinions, values, attitudes towards the subject of interview conversation (Currie, 2005). Qualitative data is said to be high in validity and less and lowly on reliability. The researcher

collected primary data from the target population through use of questionnaires and face to face interviews

3.4.2 Secondary data

Secondary data- this the information which was collected in past time for different purpose and tis information is available in different forms such electronic, written and printed and published or unpublished confidential documents in various organisation. Defined secondary data that it is data that have been already collected for purposes other than the problem at hand and the information can be located quickly and less expensive. Characteristics of secondary data have been mentioned to be related with less involvement of the researcher, data is collected for other problems, collection process is rapid and very easy and lastly collecting cost is relatively very lowly.

Currie (2005) classified quantitative data into category of secondary data as this is information that has already been tested and analysed using psychometric techniques or when the results of large-scale survey has been analysed. Unlike qualitative data, quantitative data tend to be highly in reliability and lowly in validity.

The researcher had to access secondary information from the company website, company documentations and the process had to involve signing of non-disclosure of such particular information except for the purposes related to the study only.

3.5 Research Instrument

3.5.1 Questionnaire

Abawi (2013) defined a questionnaire as a data collection instrument which consist of series of questions and other prompts for the purpose of gathering information from respondents. The Questionnaire as a research instrument use series of questions for purposes of gathering information from respondents, more importantly for statistical analysis purposes, Blaxter et al (2010). Questionnaires can be divided into two types which are structured and unstructured questionnaires. Structured questionnaire has definite and concreate questions which are prepared in advance, whereas the unstructured questionnaire act as the guide more particularly in

interviews and this instrument is flexible for the researcher to ask for clarity in other responses provided.

For the purpose of this research the researcher adopted use of a **structured questionnaire** which have close ended questions. The close ended questions are in the form of lirket scale questions which have predetermined responses which respondents are supposed to choose from the stated alternatives. The researcher used mostly close ended questions which have zero property of interaction with the respondents, with the exception of few open ended open ended questions. The questionnaire was used to gather information from the internal departments of the organisation.

3.5.2 Justification of Questionnaire to research study

For the purposes of this research the research adopted to the use of questionnaire as this has been widely used as the best in tool in collecting qualitative data from the research sample. The questionnaire provides room for respondents to give their judgements of the questionable areas without the influence of the researcher or the interviewer. According to Mitchell and Jolley (2013) questionnaires provides anonymity to respondents and as such questionnaires provide honest answers from respondents relations to questions which are too sensitive in nature.

3.6 Reliability of data

Reliability of data as stated by Joppe (2002) and Williams (2007) alluded that, same results can be produced if similar use of research methodology is constantly used in the same environment. Howard (2008) concurs with the above definition that reliability is the degree to which a questionnaire will produce the same result if administered again or repeated the test-retest concept. Validity looks in to the best available approximation to the truth or falsity of propositions. The researcher can ensure reliability as assessed by Smith et al (2008) by posing that measure will produce same result which were produced by previous researches if the information is reliable for that particular research study.

In order to ensure reliability of the research instruments, the researcher used uniform questions for both management and all the employees who participated in the research study. The research made sure that all the required information which was needed for the research was clearly

explained to ensure high response rate and accuracy. According to Rudd, (2005) reliability rate ranges from 60% - 80%. To ensure clarity a pre-test was conducted by the researcher using subjects who were not part of the research sample to answer the questions which were on the research instrument so as to identify inconsistences with the instrument.

3.7 Validity

Joppe (2000) stated that validity measure of whether the research truly brings out expected results which it is supposed to bring and also to look at how truthful are the results. Howard (2008) validity measure the degree to which a questionnaire reflects reality. Byram, et al (2013) stated that validity is the extent to which test is testing what is claimed to test and it is divide in to two, that is external and internal validity. Internal validity of a research instrument is its ability to measure what it aims to measure whilst external validity focus on the generalizability.

In the research the validity was given as the average as the employees which were used are from within the same organisation. to improve validity the researcher carried out a pilot test of the questionnaires to check on responses

The researcher used a high degree of close ended questions as to open ended questions so as to ensure validity aspect has been taken in to consideration from all aspects of the research. In addition, Johnson and Christensen (2014) described close ended questions as questions which forces respondents to choose answers from already suggested opinions. Therefore, the use of closed ended questions tried to remove irrelevant responses.

3.8 Ethical considerations

Ethics in research refers to norms of conduct that differentiate acceptable and unacceptable behaviour (David and Resnik, 2011). First a letter of research was obtained at the department of management at school to PSMI to introduce the researcher and the area of research which the researcher was to conduct in relation with the organisation to seek permission to carry out the research at West Hospital a subsidiary unit of Premier Service Medical Investment. The questionnaire or the research instrument shows purpose of the research and respondent anonymity is also assured on the document. Furthermore, all documents such as professional and academic articles and other published paper and sources are duly credited and acknowledged in the reference list.

3.9 Data presentation and analysis.

Generally, data analysis is regarded as a means by which researchers search for meaning. Researchers are known of engaging their intellectual capabilities in trying to drive meaning and sense of quantitative information or raw data collected in research sample (Hatch, 2002). Center for teaching, research and learning (n.d.) defined analysis as the means by which organizing and interrogation of data by researchers to see patterns, identify themes, discover relationships, develop explanations, make interpretations, mount critiques or generate theories. The researcher stressed out the process involves synthesis, evaluation, interpretation, categorisation, hypothesizing, comparison and pattern finding.

For the purpose of this research the researcher collected information gathered from questionnaires and produced tabulates for the responses which were given by respondents. Graphical representation and diagrams were used to interrogate and analyses the operational risks which were facing PSMI as an organisation and further analyses effectiveness of existing objectives/objectives and operational risk management strategies were also put in test. Operational risk management strategies, factors of an upper hand and lower hand were recognised from the available literature and as such regard the variables were included in the research instrument.

According to Kumar (2011) data analysis is dependent upon how it was collected and the way it is intended to be used. The questionnaires after being checked to see whether they had been completed were processed to get meaning form the raw data which was collected from the field. The data was processed to come up with percentages for the responses which were given by respondents so as to giving meaningful conclusions from the data gathered. Data analysis refers to the transformation of raw data in to what makes it understandable and easy to interpret. During the analysis stage, the researcher used a computer in storing, retrieving and for the further process of the data analysis using Microsoft office suit applications such as Microsoft Word and Excel.

3.10 Chapter summary

This chapter provided an insight on the method which was used by the researcher in gathering data. Justification of the methods and tools which were used were given as well. The preceding

chapter is going to be based on the information which was collected using the techniques highlighted above. The information is both qualitative and quantitative in nature.

Chapter Four

Data presentation and analysis

4.0 Introduction

This chapter focuses on the data presentation and analysis. The chapter takes the readers through the tabulate, diagrams and graphical presentation on data that have been gathered on the sample area of the research and conclusions to be drawn through.

4.1 Questionnaire analysis

A total of 80 questionnaires were administered and sixty-five were successful returned completed thus bringing the response rate to 81.07%. The reason why some questionnaires were not returned is mainly due to lack of interest of respondents, as they deemed the topic not vital to their work thus contributing to some analysis to some extend on whether operational risk issues are either discussed in the work place or not. Table 4 below illustrate the response distribution of the questionnaires.

Table 4. – Questionnaire response rate

Respondents as per department	**Questionnaires administered**	**Questionnaires Returned**	**Response rate**
Management	4	4	100%
Accounts	8	8	100%
Billing	7	7	100%
Front-desk clerks	5	5	100%
Pharmacy	3	3	100%
Ward-nurses	21	21	100%
Catering	9	9	100%
Housekeeping	8	8	100%
Total	**65**	**65**	**100%**

The response rate of 100% is acceptable for the analysis of data which was gathered in the field to draw conclusions from. The percentage rate does represent the majority of the population basing on criteria the researcher used.

The questionnaire comprises of two sections with the first one seeking to understand the background of the respondent as well as experience and educational qualifications. This has much influence with how an individual will be able to participate on operational risk management schemes. The second section of the questionnaire looks in to questions that related to operational risk management strategies which were being used in the organisation and their effectiveness.

4.1.1 Respondents' gender specification

Respondents were asked to highlight their gender figure 1 below represents results which were obtained.

Figure 1 – Gender difference of the participants in the sample.

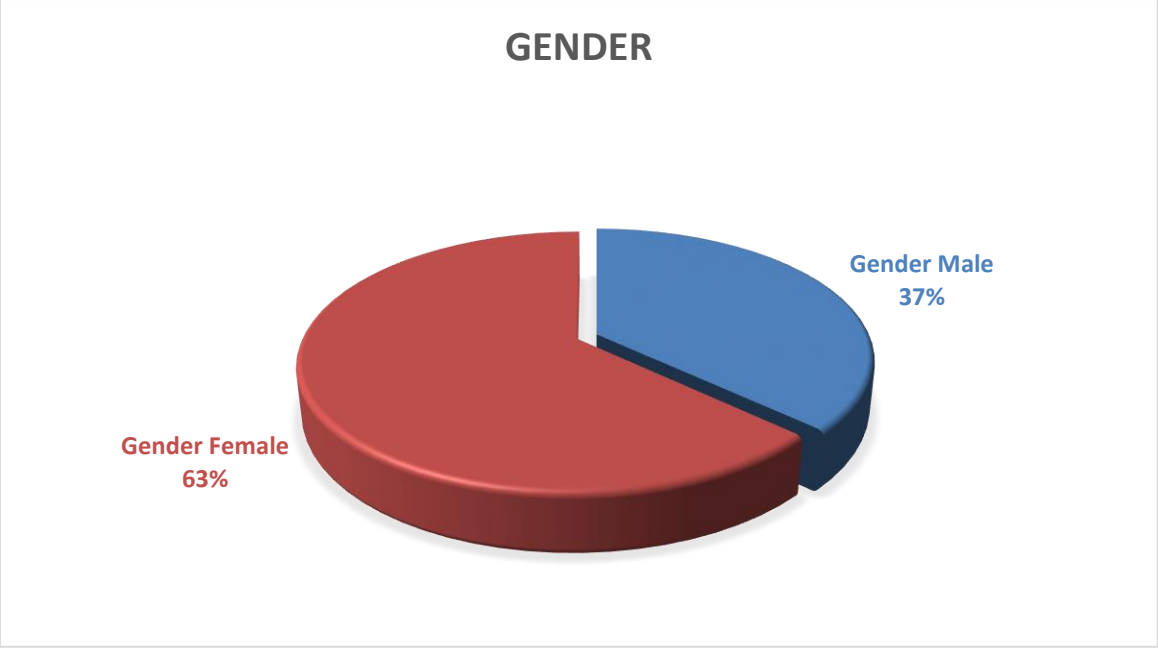


Fig 4 illustrate 63% being the percentage of female respondents who participated in the research study and 37% being a representative of males. Results have shown that the research field is a

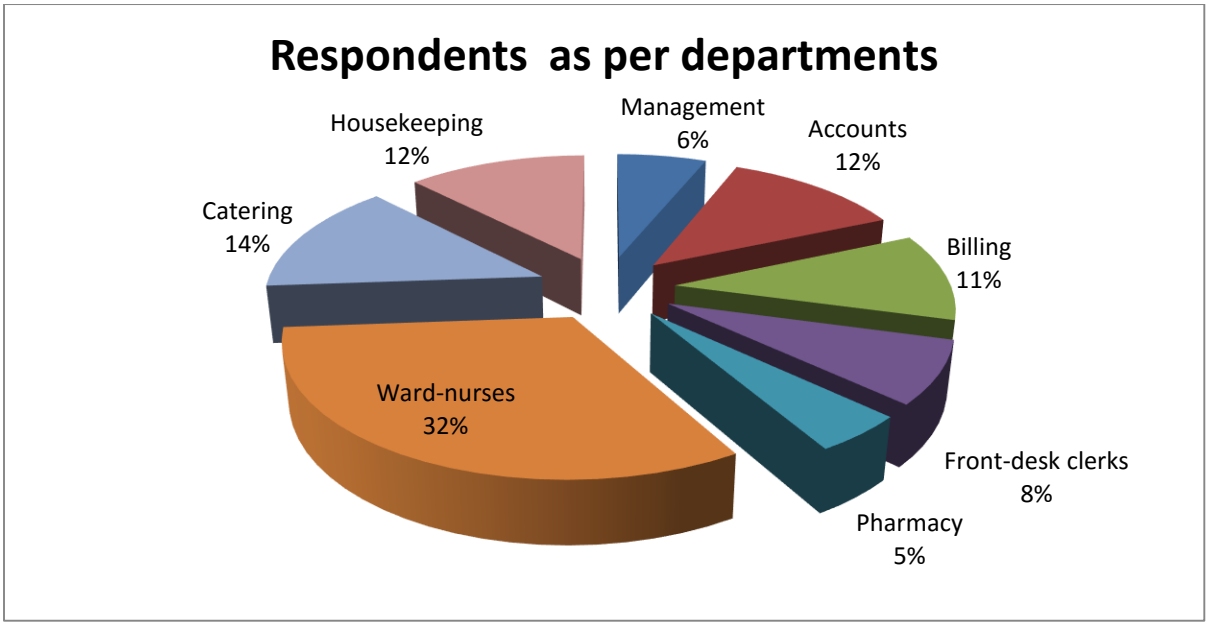
female dominated environment and as such the results reviewed also that, nursing is a female dominated field although men are joining the profession.

In the context of operational risk Franzetti (2016) concurred that cultural differences, especially with respect to morals and gender differences can lead to material losses. Taking for instance women are increasingly playing important roles of management and the author speculate that operational risk management is going to be influenced by attitudes and perceptions of women. Women in their nature or nurture are taught to be humble, passive, obedient and caring and issues to do with risk taking are not part of their socialization. Franzett (2016) also pointed out that it is uncontested that men and women differ when it comes to risk taking.

4.1.2 Area of occupation

Respondents were asked to highlight on departments in which they are attached in the organisation and figure 2 shows results of respondents to this question.

Figure 2 – Respondents number as per department



As highlighted by **fig 2** above, 32% of the respondents were nurses constituting the greater percentage of respondents, followed by catering department with 14% and 12% from the housekeeping departments despite low response rate which was noted by the researcher. Furthermore, results in fig 2 has proven that less of the employees are working in the

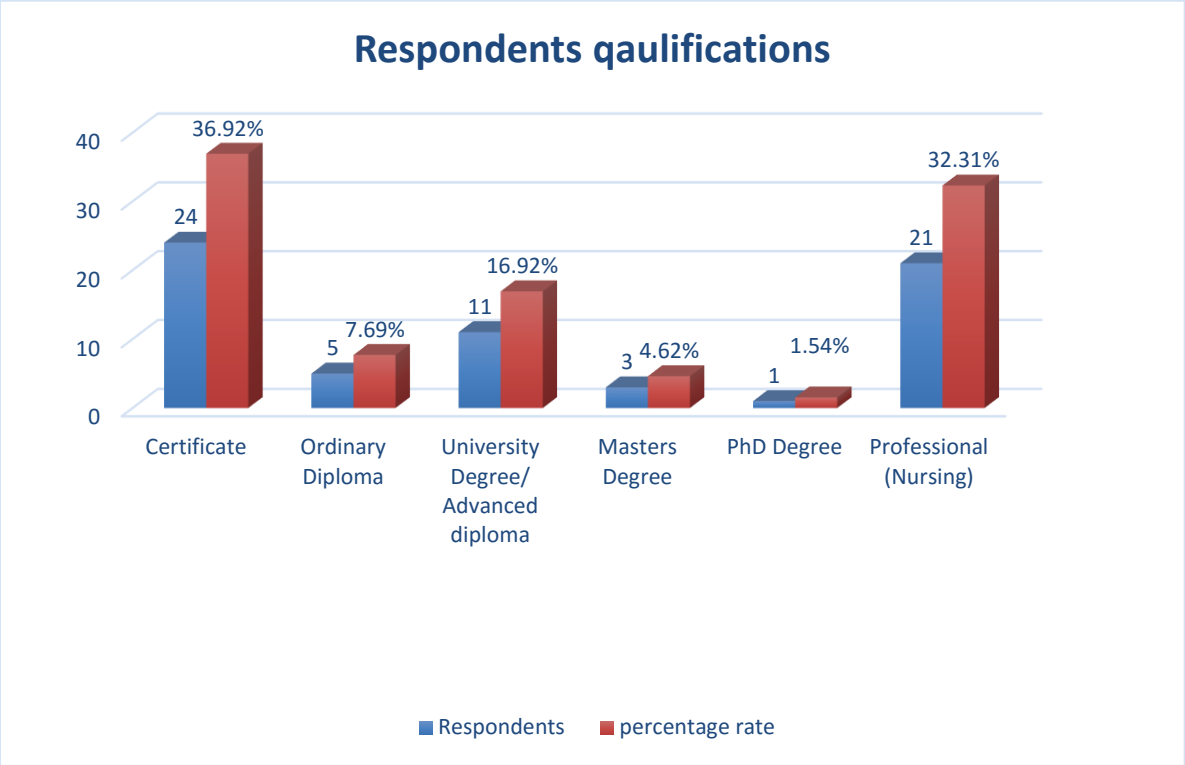
management and administrative departments and such is evidenced by 6% of management, 12% covered by the accounts department and pharmacy producing least results towards responding to the questionnaires which were provided.

According to Carroll (2011), some departments in the organisation are more exposed to operational risks due to their nature of activities which are carried in those departments. The extend of exposure can be described based on the extend of hands on activities and the complexity of systems which are used in processing activities.

4.1.3 Educational qualification of respondents.

Questions on academic qualification were directed to respondents to highlight on their highest level of academic knowledge and figure 3 below highlights the results which were obtained in that regard.

Figure 3 – Respondents' academic qualifications



Out of a total of 65 respondents in the sample 24 respondents are carrying certificates there by constituting 36.92% of the total sample. 32.31% have certificates in the nursing field, followed

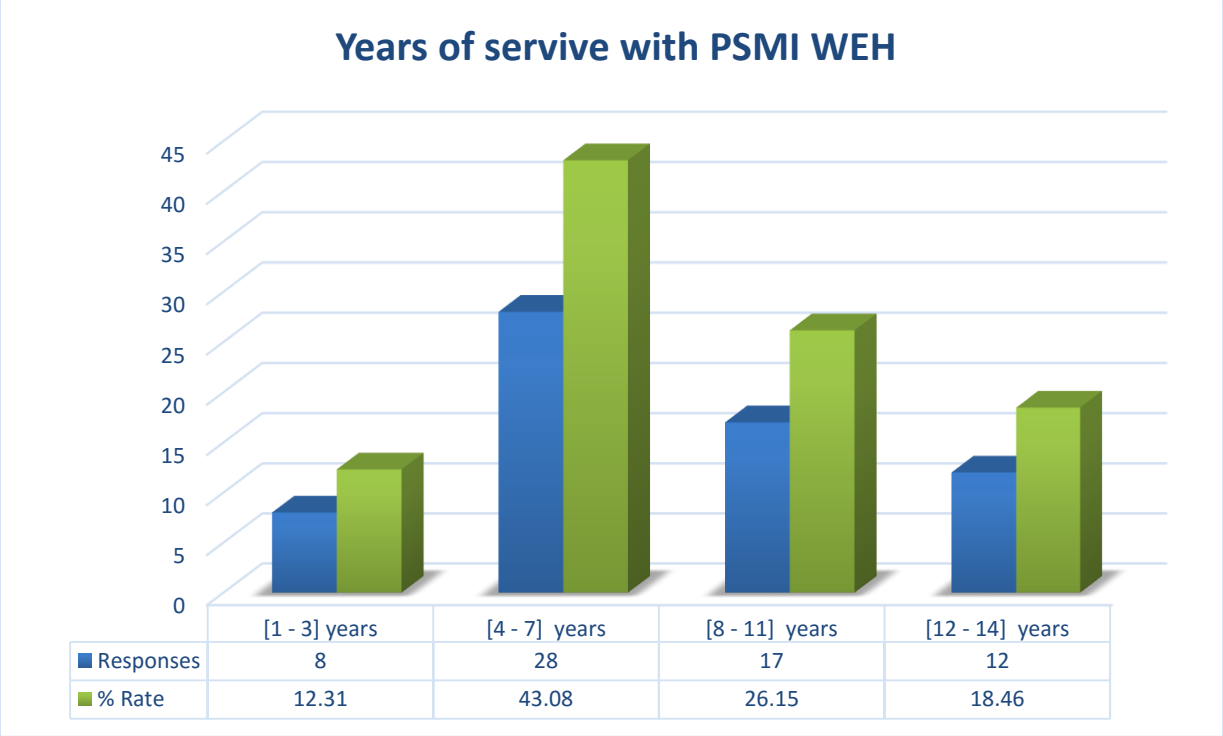
by 16.92% of the respondents who have at least a degree in different from programs or an advanced diploma. In the administrative department among managers there is 1 individual who has got a PhD degree and 3 individuals who have masters' degrees in different disciplines.

Danielson and Scott (2009) agreed that one's level of academic is a key necessity to the implementation of policies and understanding of what are operational risks and their implication to the company. As such all respondents have academic knowledge which will enable them to give responses which can be relied on.

4.1.4 - Years of service with the organisation

Participants were asked to indicate their length of services with the organisation by placing a tick in the ranges which were provided. All 65 respondents answered the question successfully making it a 100% response rate. Below is a diagram is a diagram highlighting results which were gathered.

Figure 4 – Period in which respondents spend with the company.



The research findings review that most of the participants' working experience in the organisation fall in the range of 4 – 7 years, there by constituting 43.08% of the total sample. Following are 17 participants who reviewed that they have served with the organisation for period in between 8 – 11 years, 18.46% represents employees who had served with the company since its commencement of operations in 2003. Lastly is a group of new employees who participated in the research there by constituting 12.31% of the total responses which were gathered in the field.

Period of service is very important in determining level of understanding of a respondent in relation with the organisational rules and regulations. According to Storkey (2011) operational risk can be easily identified an assessed by an individual who has been in the system of the organisation and a person who understand all the protocols which are set in management of activities in the company,

4.1.5 Positon held by respondents.

Participants were also asked to highlight their positions in departments they are attached. Such information this help the researcher with different responses that will help in coming up with precis answers to the subject matter. Table below shows number of respondents and their hierarchical position in the company.

Table – 5: positions level of the respondents

Position	Respondents	Total %
Director	1	1.53%
Manager	3	4.62%
Supervisor	19	29.23%
Operational staff (low level staff)	42	64.62%

Operational staff constitute greatest percentage of participants with 64.62%, that is 42 responded that they are operational staff of the total population, followed by 29.23% of supervisors who are part of departmental heads and team leaders when it comes to nurses in different wards of the

hospital. 4.62% represents part of manager at the hospital with 1 director who is the Head of the hospital who also took part in the research.

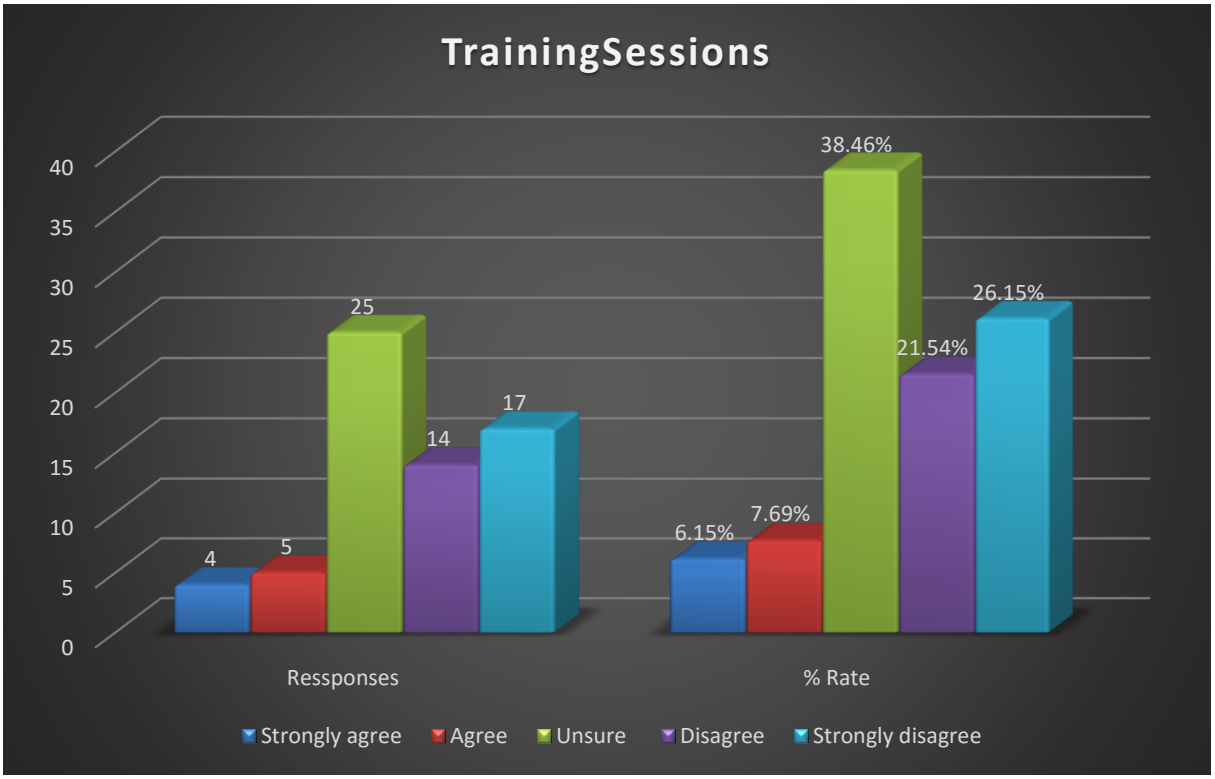
The researcher cantered more efforts on operational staff as these are the employees who are affected by much risk exposure since they are involved in the day to day hands on operations of the organisation in various department they are attached in the company. The same notion has been supported by Carroll (2011) who mentioned about departmental differences in operational risk exposures.

Section B of the questionnaire focused on information on operational risk management strategies

4.2.1 Training sessions of operational risk

Respondents were asked to answer on whether, they are trained on issues concerning operational risks in the organisation. Below is **Figure 5** summarising the findings

Figure 5 – Training sessions



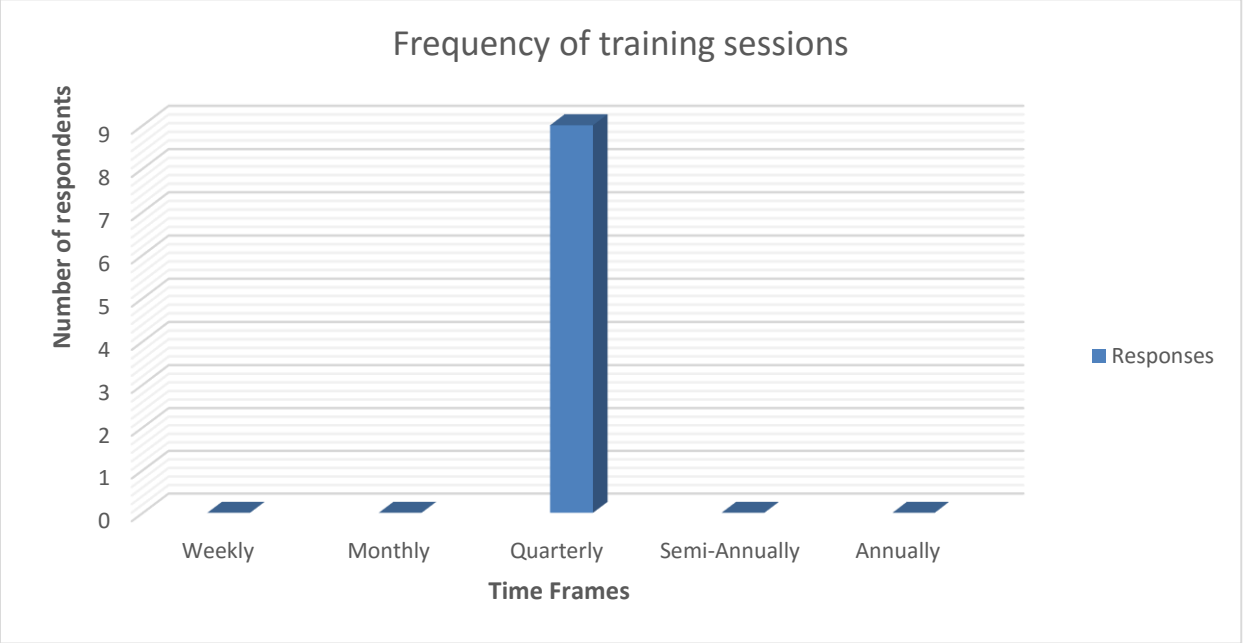
As outline in **fig 5** above, 9 respondents concurred that operational risk training sessions are conducted in the organisation and these respondents are represented by 4 participants who strongly agreed and 5 who agreed to the notion and totalling a magnitude of 13.84%. of the total participants 38.46% were unsure if these training sessions are conducted in the organisation and 21.54% and 26.15% disagreed to the notion that operational risk training sessions are conducted in the organisation.

Tattam (2011) argued that for an organisation to effectively manage operational risk training is the starting point, so as to bring light to every member in the organisation on the subject matter. A greater number of respondents were uncertain on whether operational risk management training sessions are even provided by the organisation and this then can describe the level of understanding of the employees when it comes to risk management issues.

4.2.2 Frequency of training sessions at the organisation

Participants were asked on frequency of how training sessions are conducted and the diagram below summaries the findings which were given.

Figure 6 – Responses on frequency of training sessions



As **fig 6** illustrates, 9 respondents only respondent that training sessions are conducted quarterly. Thus making 13.85% response rate. Response rate on this question turned out to be very low as most of the responses which were given on whether the operational risk sessions are conducted in the organisation dominated on the uncertainty of respondents and some strongly disagreed to the notion in **fig 5** above.

4.2.3 Existence of an internal control department and operational risk management policy.

Respondents were asked to indicate if the organisation have an internal control department and to highlight if the department have an operational risk policy document which governs management of risks in the organisation. Table below summaries results which were obtained.

Table 6: summary of responses which were given in regard to the question.

	Existence of internal control dept.		**Existence of ORM policy document.**	
	Responses	**% Rate**	**Responses**	**% Rate**
Strongly agree	18	27.69%	0	-
Agree	32	49.23%	5	7.69%
Unsure	15	23.08%	16	24.62%
Disagree	0	-	26	40%
Strongly disagree	0	-	18	27.69%
Totals	**65**	**100%**	**65**	**100%**

Table 6, summaries the findings and it is clearly illustrated that 27.69% strongly agree and 49.23% concurred that the organisation has got an internal control department. However, 23.08% or the respondent were not sure if the organisation has got an internal control department.

It can be concluded that 77% of the participated agreed that sure an internal control department does exist in the company and this is supported by Nikolai (2009) and Hightower (2008), who stated that a company should own an internal control department which act as the control centre of all activities in the organisation.

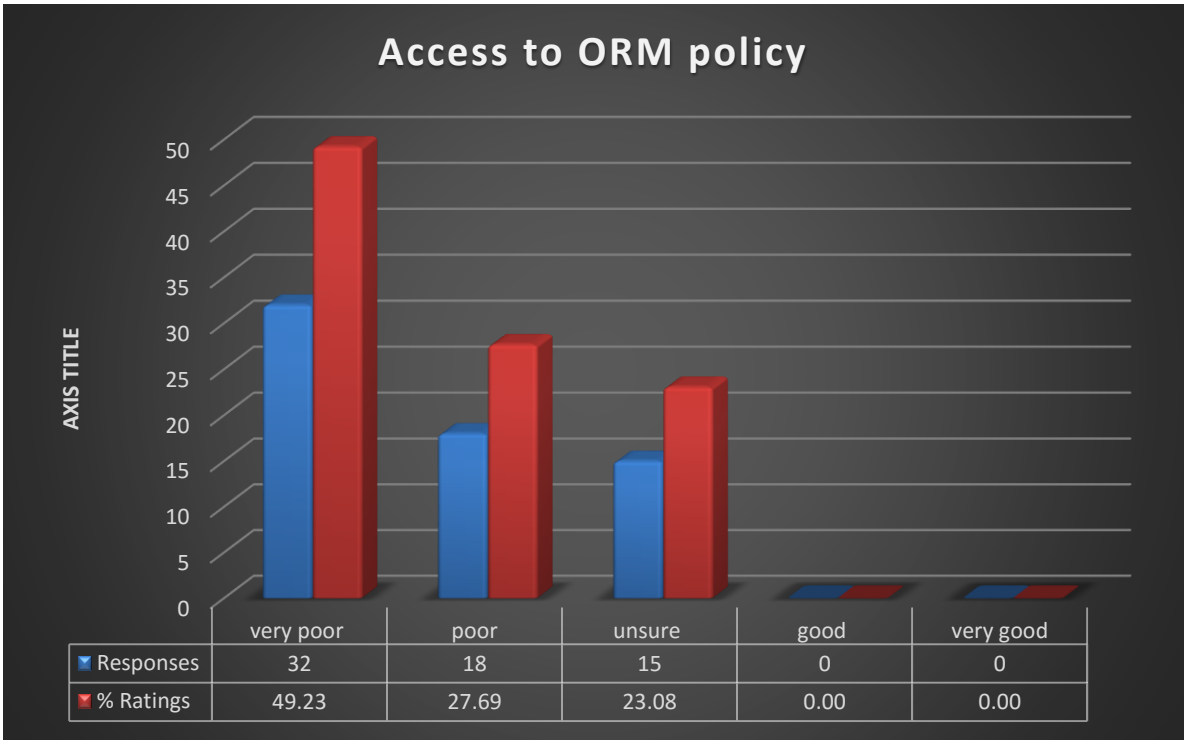
Furthermore, on the second part of the question which the researcher was examining on whether the internal control department has got a policy which governs matters related to operational risk, 40% of the respondents disagreed and 27.69% strongly disagreed to the notion. Only 7.69% of the total sample were unsure the internal control department has an operational risk management policy document.

Masenene (2015) stated that to effectively manage operational risk an organisation should be guided by an internal operational risk management framework which is set by the board and management of the company. The results which were gathered from the research sample showed respondents were not sure if the internal operational risk management framework exist or does not exist. If the policy document exists, it can be proven by the results that not every employee in the organisation is aware of the document and what it serves.

4.2.3 Easy of access to the policy document.

Respondents were asked on their take on easy of accessibility of the internal framework on operational risk management. Figure 7 below outline the overall results

Figure 7 – Access to the ORM policy document.



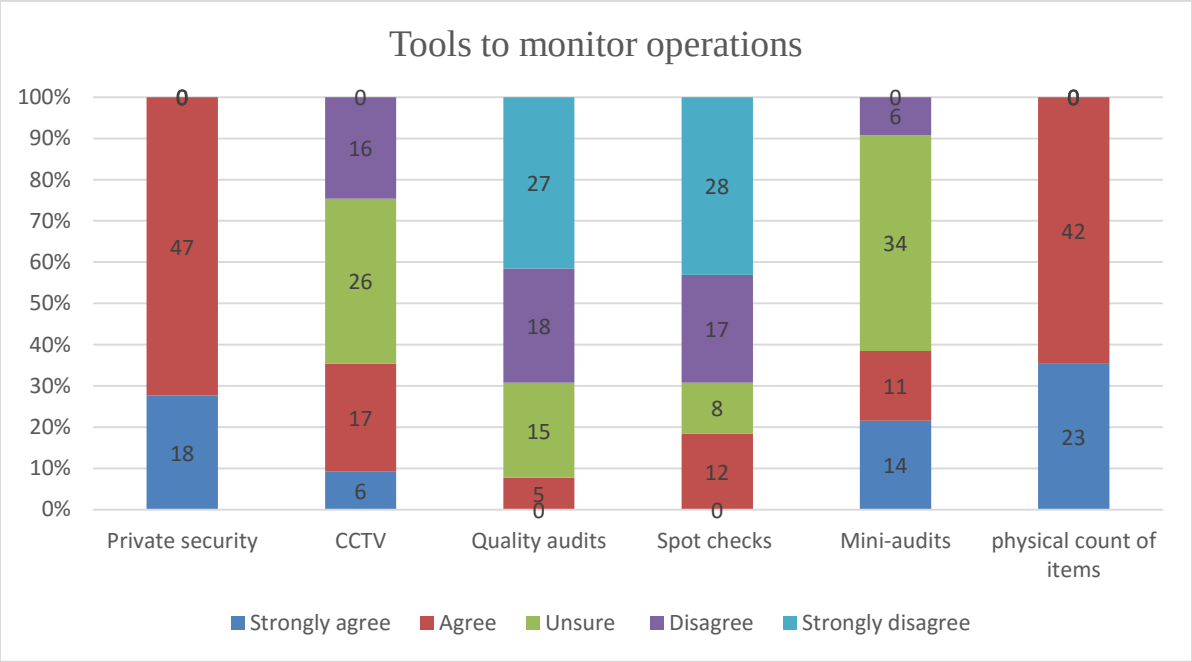
According to **fig 7** above, 49.23% of the participants rated very poor on easy of access of the internal framework that focuses on operational risk management. Additionally, 27.69% rate poor on the rankings tables as shown whilst 15 respondents were indecisive to the notion,

Hopkins (2017) who stated that for a company to manage operational risk, it should formulate policies and manuals which are meant to provide guidance on management procedures to be followed and these policies should be communicated to all members of staff. It is therefore proven by the results that the internal framework is not known by all as being showed by results from **fig 7** and responses which were gathered in **Table 6** above.

4.2.4 Monitoring as a strategy towards operational risk management

Respondents were asked on tools which are used to monitor operations in the company. Summaries of the findings are shown in **figure 8.**

Figure 8 – Tools to monitor operations in the company



According to **fig 8** above, 27.69% strongly agree that private security is used in the organisation for monitoring activities and also 47 respondents (72.31%) to the total sample agreed that private security is surely used to monitor actives in the organisation.

Use of private security as part of monitoring operational risk was supported by Storkey (2011) who argued that monitoring take third stage of operational risk management and as such monitoring and report should be a continuous process.

Fig 8 also shows that 9.23% strongly agreed to use of security cameras and 26.15% agreed to use of CCTV in the organisation. However, 40%o the respondents were indecisive of the notion with 24.62% disagree to use of security cameras in monitoring activities in the organisation.

Therefore Hall (2003), argued that security cameras are part of the first line defense, in control structure to prevent unwanted events. As such conclusions, can be drawn from the data that some security cameras are concentrated to some parts of the organisation and some areas lacks the facility. This is being evidenced by some responses agreeing to use of security cameras but with their response rate being outweighed by those that indefinite if the company uses CCTVs for monitoring operations.

Fig 8 outline that 41.54% strongly disagree that quality audits are conducted in the organisation and 27.69% disagree as well to the notion. From the total sample 15 responded that they were unsure if the quality audits are conducted thus representing 23.08%. However, only 7.69% of the total sample concurred that quality audits are carried out in the organisations as a means to monitor risks associated with quality matters.

It can be concluded that, majority of the responses showed that quality controls are not used as measure to monitor quality in the organisation. As advised by Javier (2017) quality controls are of great importance if the organisation is to reduce its exposure of operational risks through self-assessment so as to check either frequency and loss of severity. This can be used as a basis for quality inputs and processes which can be used to produce quality end results or output.

According to **fig 8**, 52.31% of the respondents were uncertain if mini-audits are conducted in the organisation and 6 participants strongly disagree to the notion thus, representing 9.23% of the total sample. However, 16.93% agree that mini-audits are conducted and 21.54% are also in agreement that internal control department conduct mini-audits to monitor activities in the organisation.

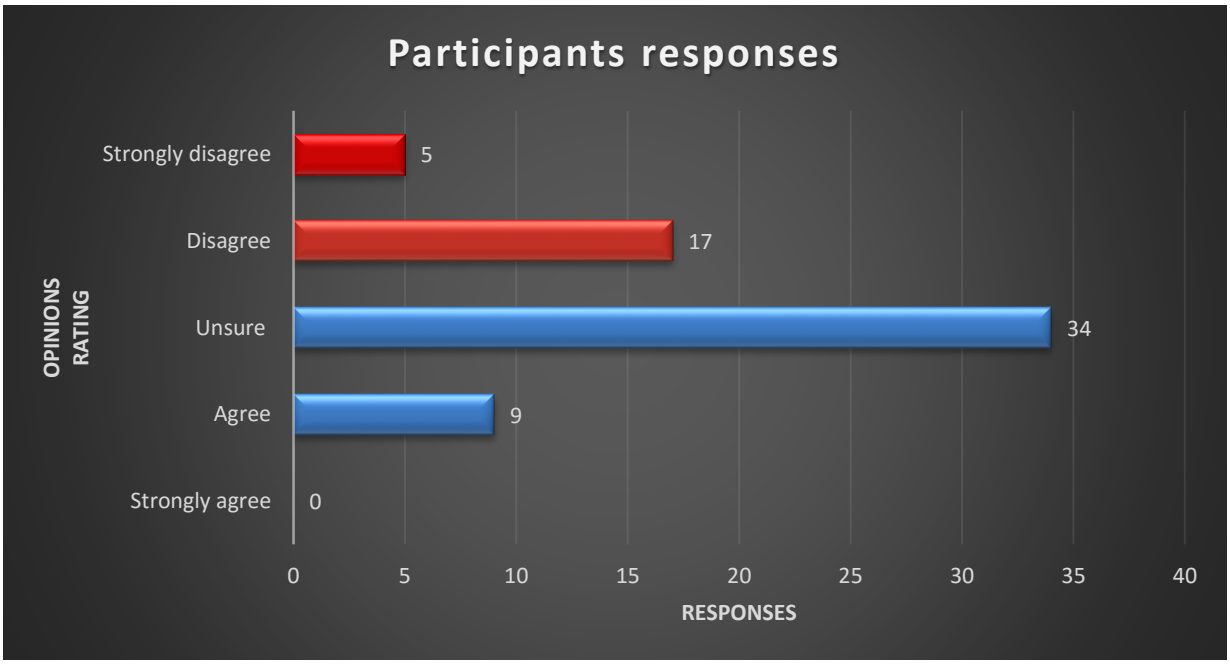
On the basis of a majority, it can be concluded that mini audits sessions are not being done, and thus poses a challenge on how best the organisation can manage overall operational risks in the company. According to Turner (2016) mini-audits are part of the detective internal control measures which can be adopted by the organisation if it is to hedge itself against operational exposure cost effectively.

Fig 8 outlines that 35.38% strongly agree and 64.62% were in agreement with the notion that physical counts are carried out as part of monitoring activities in the company. The stock counts are carried out on monthly basis in the organisation, and high value items including vials are counted during the sessions. This position is supported by King (2011) that spot checks are used to check high valued items and this process in under detective internal control provision and it is effective in reducing or eliminate cases of theft and deceptions.

4.2.5 Risk assessment session

Questions were directed to respondents on whether there are operational risk assessments carried out in the organisation. Figure 9 below, illustrates the findings.

Figure 9 – Responses to risk assessment question



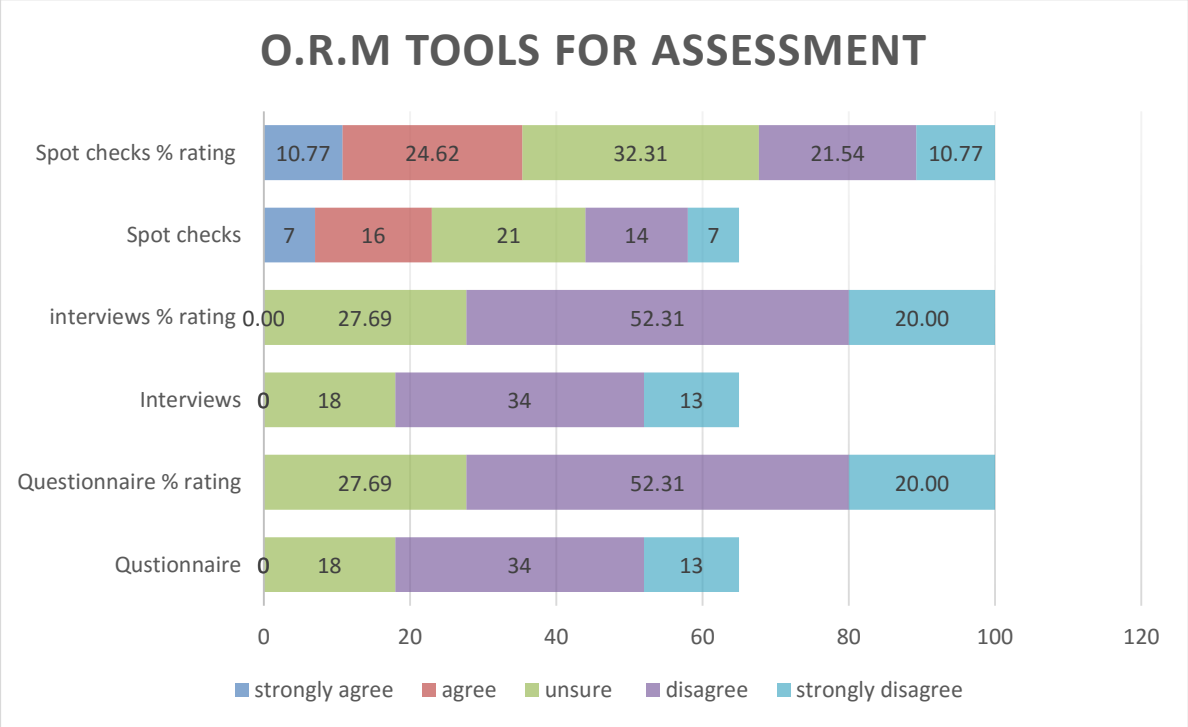
As outlined by **fig 9**, the majority of the respondents were not sure if there are any risk assessments taken in the organisation thus representing 52.31% of the total, 7.69% strongly disagree and 26.15% also agreed to the view that such sessions are ever conducted in the organisation. However, 9 respondents concurred that assessments on operational risk are conducted in the organisation and their representation only constituted 13.85%.

Basing on the majority, 62% can conclude that risk assessments are not conducted in the organisation. However, Hull (2010) was of an opinion that risk assessment is an important component of operational risk management and as such assessment should be exercised in the organisation, if effective risk management process is to be achieved. Jorion (2007) concurs with the notion, stating that critical assessments will provide information related to expected frequency of operational risks.

4.2.6 Justifying tools which are used for operational risk management process.

Respondents were asked to answer on whether the mentioned tools by the researcher are even used in the company, during risk assessments sessions. Figure 10 below summaries the findings.

Figure 10 – justification of operational risk management tools



As per fig 10, 52.31% of the respondents disagree to the notion that questionnaires are used in the company to assess risks, 27.69% of the participants were indecisive whilst 20% strongly disagree.

Research findings showed that questionnaires are not part of the assessment tools which are used in PSMI. Despite their effectiveness on providing accurate data as argued by Javier (2017) the company is not using the instrument for self-assessment on quality of internal control procedures

Furthermore, **fig 10** show that same results which were obtained from responses provided by participants are similar. Concluding that questionnaire and interviews are not part of instruments which are used to assess the extend and positions in which potential risks can be identified.

Fig 10, also show that 10.77% strongly agree to the notion that spot checks are conducted when assessing operational risk and 24.62% were in agreement as well. 32.31% were indecisive whilst 21.54% and 10.77% disagree and strongly disagree respectively.

Conclusions can be drawn that spot check are used in some section of the operating functions of the company, particularly in administrative works in which such sessions are conducted in areas where cash holdings are involved.

4.2.7 Recording systems, insurance and incentives towards ORM.

Questions were directed to participants to give their views on whether the organisation have recording systems which are used to capture data on operational risks and also to check on whether there is an insurance policy which covers employees if they are injured at work. More so participants were asked to provide responses on issues concerning packages attached to operational risk identification within the internal control systems.

Figure 11 below summaries the research findings.

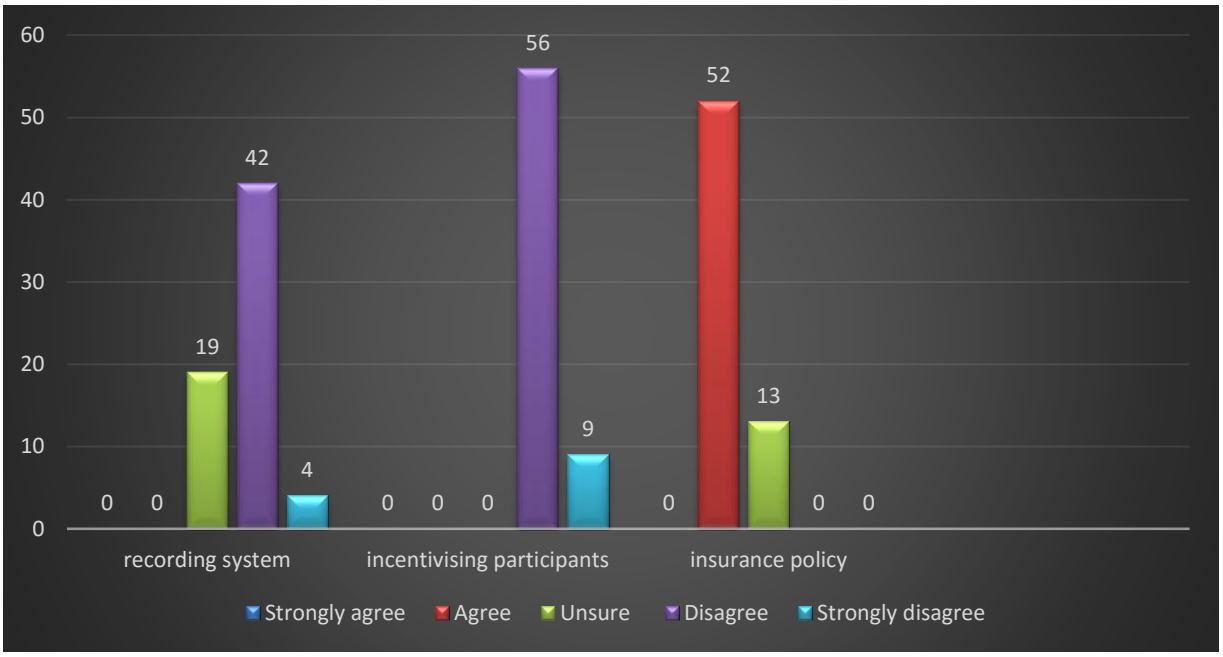


Fig 11, illustrate that 42 participants constituting 64.62% were in disagreement with the notion that the organisation has got a facility where operational risk events are recorded whilst 35.38% represented by 19 participants were indecisive. Operational risk management issues are not part of the organisational culture as being evidence by the results that there are no systems which are used to record data.

According to BIS (2002) outlined that data collection and analysis require technical equipment and time investment in the process and as such this start with building systems which are used to record and document information related risks which are identified during work operations.

Fig 11, also show that 86.15% of the participants could not agree to any packages being granted to individuals who have identified potential risks with the company's processes and 13.85 strongly disagree as well.

For workers to actively involved in operational risk management process Lawton et al (2015) stated that management should incentivize employees who would be actively participating and showing good conduct towards management of operational risks. The statistics at PSMI Westend Hospital are showing a complete different set-up to the notion of incentivizing of staff.

As per **fig 11**, 80% of response on question which was investigating whether the company has an insurance policy which covers employees when they are injured whilst they are at work produced positive results respondents agree, although 13 of the participants were not sure.

Koller (2011) supported that companies can hedge against risk through use of insurance houses, and also that insurance houses or companies offer health insurance services packages which are meant to cover medical issues related to employees. The results showed that the company is aware of potential risk which might be caused by operational functions and processes and that can be justified by the fact that the company hedge itself against such costs by use of an insurance policy that covers employees.

4.2.8 Actions which are taken when employees fail to observe rules and procedures

Respondents were asked to indicate on actions which are taken when an employee fail to observe operational procedures in his or her conduct.

Table :7 – Summary of research findings

Course of Actions	Number of respondents' agreement	% Ratings
Contract of employment terminated	23	35.38%
Write reports and no further action is taken	52	80%
Fined (monetary value)	0	-
Prosecuted	16	24.62%

Responses which were gathered in the research study indicate that when procedural rules are broken by employees asked to provide written reports are often. This evidences by 80% of the target population concurring to that form of resolving issues. 35.38% concurred to termination of contracts and 24.62% reported that cases can be prosecuted. However, no findings were evidenced on fines attached to breaking of procedural rules of the organisation.

4.2.9 Resources to manage operational risk

Questions were asked to participants to provided their view on whether the organisation has got adequate resources to manage operational risk in the company Figure 12 show results.

Figure 12: Resources to manage operational risks

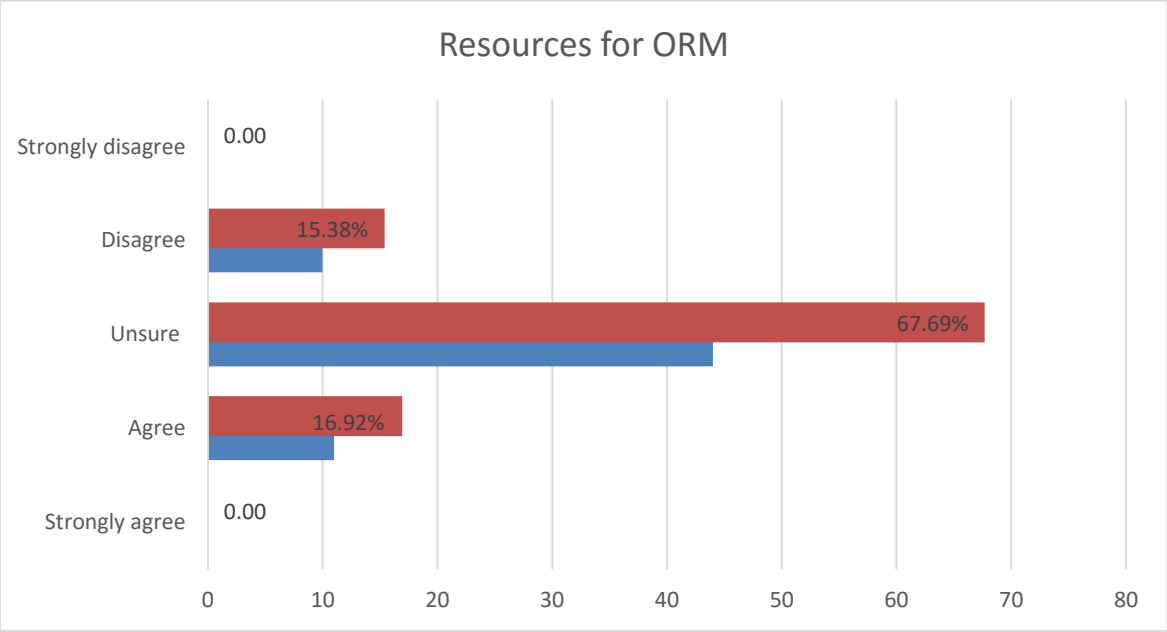


Fig 12, above show that 67.69% of the participants were uncertain towards the notion that the organisation is in a position to provide more resources on operational risk management, 15.38% disagree whilst only 16.92% agree that the company is equipped to manage operational risks.

According to HKIB (2013) stated that for an organisation to effectively manage operational risks, resources are the key drivers to the management process. Cited resources include; human capital, advanced information systems and financial resources taking the lead. The statistics basing on the responses which were gathered showed that PSMI Westend Hospital is lowly capacitated in terms of financial resources.

4.2.10 Reasons leading to failure in operational risk management

Most of the responses which were cited by participants related to financial constraints. More sited that it is impossible for the organisation to channel resources towards management of operational risks or even to invest in systems which will help it to manage such risks as the company is failing to pay back dated salaries.

4.3 Summary

This chapter focused on data presentation and analysis of the data which was gathered through use of a questionnaire. The results were presented using tables, pie charts and graphical presentations. Analysis of data was given in a descriptive nature and the following chapter will focus on summary of the findings to the research.

Chapter Five

Summary, conclusion and recommendations

5.0 Introduction

This chapter focuses on a brief summary on conclusions and recommendations which were drawn from literature in line with study. The chapter also provide major research findings based on results which were drawn from the study and recommendations of the researcher. Lastly the chapter sums up by giving insights on areas of further research.

5.1 Summary of findings

Brief summary on research findings are discussed in this section highlight results of the objectives of the research study.

i. It was noted that the organisation does not own any operational risk management policy which governs operational activities and risks which are associated.
ii. Training of staff on matters concerning operational risk was noted to be lacking in the company and yet the company's operations are associated with several risks which are driven from day to operations of the organisation. operational risk management should be everyone's responsibility and to achieve that training sessions are the means to empower every staff member of the organisation.
iii. The results reviewed that PSMI Westend Hospital lacks facilities which are used to record information on operational risks within their operations.
iv. The available control which are at PSMI Westend Hospital are not robust enough to encounter operational risk which are affecting the company as a whole.
v. A culture of risk management in all aspects have been noted to be lacking in the company as there is no initiation which is done by management to develop it.
vi. Monitory issues in the company were also cited in the findings to be the major restraining issues toward developing and adoption of modern operational risk management systems despite the weakness which were also evidenced in the existing internal controls the company is using.

5.2 Conclusions

The research achieved its goals of focusing on how operational risks and the management process can be used to come up with sound business entities trading in the healthcare system. The organisation should thrive to put operational risk control measure in its daily operations and implement monitoring measures to ensure that goals of the organisation are achieved in a costs and effective manner.

It was found that PSMI Westend Hospital doesn't have an operational risk management framework, which is a document that can help the organisation with how best it can identify types of risk and the extend of severity of the risks. The research findings showed that there is need for the formulation of a policy document which can be communicated to every member of the organisation on the importance of the operational risk management and the roles of every member in to ensuring that success of organisational goals being free risk exposure is achieved.

The organisation can also invest in hiring of experts in identification, designing of processes with less risk exposure and training of staff such that every member of the organisation will have an understanding of his actions against risk exposure.

5.3 Recommendation

The recommendation provided are meant to help organisation in the healthcare system with how best they can manage operational risks which are derived from daily operations of the business.

5.3.1 The board of directors and management should integrate its planning system together with the operational risk management philosophy such that risk strategic risks which are derived from the planning process are reduced. That will further assist in mitigating risk which affects the business on daily basis. Approval strategies should be made after considerations of potential risks associated with the plans.

5.3.2 Creation of awareness on causes and sources of operational risk to the organisation's functional departments will also help the organisation to reduce its financial costs which is incurred during the process of correcting the damages. The awareness should be prepared on the premise that it will provide identification, assessment, control and provision on reports for easy management of operational risks.

5.3.3 To ensure effective management of operational risk, investments in technologies that assist in monitoring and controlling of the operations will should be made possible by the board of directors as they are the overseers of the organisation. Technology has been proven to be cost effective in various ways and that the same with reducing operational risk which deter the organisation from achieving its goals

5.3.4 Training of staff is another important role in ensuring effective management of risk in the organisation. Operational staff in most cases are the first individuals to detect incidents as such they should be trained on what to expect when risks tend to happen and how to conduct themselves and ensuring that corrective actions are made.

5.3.5 The company management should invest in building formal contractual relationships with vendor of essential inputs to the process of the organisation such that each member in the relationship knows the importance or role of its services dependent to the other part. This reduces disruptions and enhance preparedness of the organisation to encounter operational risks which are brought by short production runs.

5.4 Areas of further study

Research can be done on other risk management strategies focusing on management of al operational risks which affect healthcare system which needs to be quantified such that the extend of severity or impact of risks of operational nature can be understood by all staff even those have less knowledge on administrative function particularly nurse and doctors as their field does not allow them to comment on financial implication of their actions.

Reference list:

Abawi,K. (2013), *Data collection instruments (Questionnaire and interview)Geneva: Geneva worlshop*

Andersen, T. J., Garvey, M. and Roggi, O. (2014) *Managing risk and opportunity: the governance of strategic risk-taking* Oxford: Oxford University Press.

Baker, H. K., Singleton, J. C. and Veit, E. T. (2011) *Survey research in corporate finance: bridging the gap between theory and practice*. Oxford: Oxford Univ. Press.

Bank for international settlement (2002), 'Sound practises for the management and supervision of operational risk'

Banking Policy and Regulation Department (2014) 'Implementation of operational risk management Framework'

Braga, C. A. P. (2010) *Sovereign debt and the financial crisis: will this time be different?* Washington, D.C: World Bank.

Carroll, R. (2011) *Risk management handbook for health care organizations* San Francisco: Jossey-Bass.

Carroll, R. (2011) *Risk management handbook for health care organizations*. San Francisco: Jossey-Bass.

Chamukure, C. (2015)

Chamukure, C. '81 companies closed down' *Zimbabwean Independent*, available at: https://www.theindependent.co.zw/2016/05/06/55734/ (accessed 13 January 2017)

Christoffersen, P.F. (2012) *Elements of financial risk management*, 2nd edn, Oxford: Academic Press.

Coleman, L. (2009) *Risk strategies: dialling up optimum firm risk*. Farnham: Gower.

Creswell, J. W. (2013) *Research design qualitative, quantitative and mixed methods approaches*, London: Sage Publications

Darling, P. (2011) *SME mining engineering handbook.* Englewood, CO, USA: Society for Mining, Metallurgy, and Exploration.

Dun, K. and Bradstreet, D. (2007) *Financial risk management,* New Delhi: Tata McGraw-Hill.

Duttge, G. and Lee, S. W. (2011) *the law in the information and risk society. Gottingen*, Germany: Universities Gottingen.

Elliott, T(2010) *Contingency plan and Business continuity Management*. San Francisco:Jossey-Bass

Eweje, G. (2014) *Corporate social responsibility and sustainability: emerging trends in developing economies*. Bingley: Emerald.

Feinberg, F. M., Kinner, T. and Taylor, J. R. (2012) *Modern Market Research: Concepts, Methods and cases* Washington: Cengage Learning

Flammini, F. (2012) Critical infrastructure security: assessment, prevention, detection, response. Southampton: WIT Press.

Franzetti, C. (2016) *Operational Risk Modelling and Management* Zurich: CRC Press

Fraser, J. and Simkins, B. J. (2010) *Enterprise risk management*. Hoboken (NJ): John Wiley & Sons.

Gelinas, U. L. (2017) *Accounting Information Sytems*. : South-Western.

Greenland, S. (2005) Target population. Encyclopedia of Biostatistics 8, University of California, Los Angeles, CA, USA

Grimes,D.A. and Schulz, K.F.(2002) *Descriptive studies: What they can and cannot do*, Toronto:The Lancet Publishing Group

Gupta, A. (2016) *Risk Management and Simulation*. London: CRC Press.

Harrison, J (2013), 'Some factors generating operational risk: Internal factors -those with your control'. Available at http:// www.blogs.sap.com (accessed 20 March 2017)

Hastings, N. A. J. (2015) *Physical asset management: with an introduction to ISO55000.* Cham: Springer.

Health Service Executive (2008), 'Quality and risk measurement standard', available at: http://www.hse.org (accessed 31 March 2017)

Hong Kong Institute of Bankers (2013) *Operational Risk Management* New Jersey :John Wiley & Sons

Hong Kong Institute of banks, (2013) *Operational risk management* Hoboken: John Wiley and Sons

Horcher, K. A., (2005), *Essentials of financial risk management* Canada:John Wiley and sons

Hull, J. (2015) *Risk management and financial institutions.* Hoboken: Wiley

Hull, J. C. (2010) *Risk management and financial institutions*. Boston, MA: Pearson/Prentice-Hall.

Humphreys, T. (2016) *Implementing the ISO / IEC 27001 ISMS standard*. Boston: Artech House.

Israel, G. D. (2007) *Determining Sample Size*: Florida University.

Javier, P. C. (2017) *Financial Risk Management: Identification, Measurement and Management*. Cham: Springer International Publishing.

Kawaza, K (2016) '150 companies shut shop in 2016 second quarter' *Zimbabwean Independent,* available at https://www.theindependent.co.zw/2016/07/01/150-companies-shut-shop-2016-second-quarter/ (accessed 13 January 2017)

King, M A. (2011) I*nternal control of assets: A controller and Auditor's guide* Hoboken, NJ: John Wiley and Sons

Knupfer, N.N and McLellan, H. (1994), *Descriptive Research Methodologies,* Publishers Kansa State University

Koomson A, (2011) *Operational risk management and competitive advantage in the Ghananian banking industry*, Kumasi: Kwame Nkrumah University of Science and Technology.

Kothari, C.R. (2004) *Research Methodology-methods and techniques* 2nd edn, New Delhi : New age international (P) Limited Publishers

Kotter, M. (2011) *Life Insurance: Risk management essential*. London: Springer sciences and mathematics

Koumdabagil, J (2007) *Risk Managemnt in electronic banking* Singapore: John Wiley and Sons

Lam, J. (2014) *Enterprise risk management: from incentives to controls*. Hoboken: John Wiley & Sons, Inc.

Lavrakas, P.J. (2008), *Encyclopedia of Survey Research methods* 2nd edn Los Angeles: Sage Publications

Lawton, H., Wal, Z. and Huberts, L. (2015) *Ethics in public policy management a global research companion.* London: Routledge.

Lewis, N. D. C. (2004) *Operational risk with Excel and VBA: applied statistical methods for risk management.* Hoboken, NJ: John Wiley & Sons, Inc.

Lodico, M.,Spauding, D and Voegtle, K. (2006) *Method in educational research: From theory to practice*. San Francisco :Jossey- Bass.

Mark.D, A. (2008), *Operational risk management: A case study approach to effective pinning and response* New Jersey:John Wiley and sons,

Mitchell M. L, Jolley M. J (2012) *Research design explained 8th* edn:Washington Cengage Learning

Mitchell, M. L. and Jolley, J. M. (2013) *Research design explained.* Belmont, CA: Wadsworth, Washington: Cengage Learning.

Muyambo, D. T (2016) An investigation of the debt management practices on the performance of Premier Services Pharmaceuticals. Gweru Midlands State University

OBICCI, P. E. (2017) Risk management strategies in public- private partnerships SI: Business Sci Refer IGI

Oppong, S. H. (2013) *The problem of sampling in qualitative research*, Poland: Graduate school for social research

Ott, L. R, Micheal, T. L. (2012) *An introduction to statistical methods and Data analysis 6th* edn Washington:Cengage Learning

Plunkett, W. R, Allen, G.S. and Attner, R.F. (2012) *Management* Washington: Cengage Learning.

Rai, A. K (2012) *Customer relationship management: Concepts and cases* 2nd edn,: New Dehli: PHI Learning Pvt, Ltd.

Resnik, D. B. (2011), *Scientific research and Public trust, Science and Engineering*

Reuvid, J (2010) *Mlanaging Business Risk: a practical guide to protecting your business* 7th edn London: Kogan Page Publishers

Robertson, D. D. (2016) *Managing operational risk: practical strategies to identify and mitigate operational risk within financial institutions.* Basingstoke, Hampshire: Palgrave Macmillan.

Soprano, A. Crielaurd, B and Piacenza, F. C(2009) *Measuring Operational and reputational risk : a practical approach* England: John Wiley and Sons

Storckey, M (2011) 'Operational Risk Management and Business Continuity Planning for Modern State Treasuries,' *Technical Notes and Manuals*, (05), p. 1.

Storkey I, (2011), *Operational risk management and business continuity planning for morden state treasury*. Sanjeev Gupta

Tattam, D. (2011) *A short guide to operational risk.* Farnam, Surrey, England: Gower Pub.

Turner, L. (2016) *Accounting information systems: the processes and controls*: John Wiley.

Zimmerman, F. (2011) *The Turnaround Experience: Real World Lessons in Revitalizing Corporations and Organizations* Los Angeles: F & J Zimmerman Co

APPENDIX A

Cover letter

Midlands State University

Faculty of Commerce

Department of Accounting

P O Box 9055

Gweru

April 2017

Premier Service Medical Investments

Westend Hospital

14 Baines Avenue

Harare

Dear Sir/ Madam

RE: AUTHORITY TO CARRY OUT RESEARCH

My name (R136968P), a student at Midlands State University, carrying out a research on ***"An assessment of the effectiveness of operational risk management practices at PSMI Westend Hospital."*** The research is in partial fulfilment of the Bachelor of Commerce Honours Degree in Business management that I am currently studying.

I request your assistance in my research by completing the attached questionnaire. Your contributions shall be held in strict confidence and be used only for academic purposes.

Your cooperation is highly appreciated

Yours faithfully

(R136968P)

APPENDIX B

Research Project Questionnaire

Instructions: Please put a tick on front of what you consider most appropriate answer

Remember there is no wrong one.

Section A: Preliminary information of respondent

Please attempt all questions and tick where applicable or fill in the spaces provided.

1. Please indicate your gender

Male	Female

2. What is your area of occupation?

Management	
Accounts	
Billing	
Front desk clerks	
Pharmacy	
Wards- nurses	
Catering	
Housekeeping	

3. What is your highest education level attainment?

i.	Certificate	
ii.	Ordinary Diploma	
iii.	University Degree/ Advanced diploma	
iv.	Masters Degree	
v.	PhD Degree	
vi.	Professional (Nursing)	
vii.		

4. Years of service with the organisation?

1 – 2	3 – 5	6 – 8	9 – 10	Other (specify)

5. Employment position held in the organisation?

Director	Manager	Supervisor level	Operation level

Section B: Information on operational risk Management strategies

1. *Does the organization provide training sessions on operational risk?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

2. *How often are the training sessions conducted?*

Weekly	**Monthly**	**Quarterly**	**Half yearly**	**Yearly**

3. *Does the organisation have an internal risk control unit that manage operational risks?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

4. *Is there an operational risk policy in your work place?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

5. *To what extend is the policy document easily accessed by everyone in the department.*
{Rate from 1 – 5, where 1 is the lowest score and 5 is the highest score}

1	**2**	**3**	**4**	**5**

6. *To what extend do you agree or disagree on that monitoring and control of risk occur in your work place?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

7. *How does the organisation monitor operations to mitigate chances of risk occurrence?*

Tools	***Strongly agree***	***Agree***	***Unsure***	***Disagree***	***Strongly disagree***
Private security					
CCTV					
Quality audits					
Spot checks					
Mini-audits					

8. *Are there operational risk assessment sessions carried out in your work place?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

9. *What methods are used to carry out the risk assessments?*

Method	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
Questionnaires					
Interviews					
Spot checks					

10. *How frequent are the operational risk reports reviewed?*

Weekly	***Monthly***	***Quarterly***	***Semi-Annually***	***Annually***

11. *Does the organisation have a system where operational risk events are recorded?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

12. *To what extend do you agree or disagree on management incentivising workers who detects potential operational risk in the organisation's operational processes?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

13. *Does the organisation have insurance policy which covers daily operational risks at your work place?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

14. *What actions are carried out if workers caught breaking organisational rules and regulations (egs. Stealing, drunk, misuse of company assets, corruption, etc)*

Course of Actions	Level of agreement or disagreement
Contract of employment terminated	
Write reports and no further action is taken	
Fined (monetary value)	
Prosecuted	

15. *Does the organisation have adequate resources to cater for operational risk in the organisation?*

Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

16. *What are the reasons that are leading to management of operational risk in your own opinion?*

_____

_____

17. *What are your **suggestions** towards management of risks affecting the organisation?*

_____

_____

_____

_____.

Thank you.