YANGON UNIVERSITY OF ECONOMICS
DEPARTMENT OF COMMERCE
MBF PROGRAMME

ANALYSIS ON OPERATIONAL RISK MANAGEMENT OF YOMA BANK LIMITED

NYAN MYINT AUNG

EMBF 6TH BATCH

DECEMBER, 2019

YANGON UNIVERSITY OF ECONOMICS
DEPARTMENT OF COMMERCE
MBF PROGRAMME

ANALYSIS ON OPERATIONAL RISK MANAGEMENT OF YOMA BANK LIMITED

Supervised by
Daw Yee Yee Thane
Associate Professor
Department of Commerce
Yangon University of Economics

Submitted by
Nyan Myint Aung
MBF II-39
MBF 6th Batch
Yangon University of Economics

DECEMBER, 2019

ACKNOWLEDGEMENTS

I especially would like to thank our honorable Prof. Dr. Tin Win, Rector of Yangon University of Economics and Pro Rector of Yangon University of Economics Prof. Dr Nilar Myint Htoo.

My deepest thanks also goes to Prof. Dr. Soe Thu, Professor and Head of Department of Commerce of Yangon University of Economics for their prudent guidelines to successful accomplishment of this thesis paper.

I would like to warmly acknowledge Daw Yee Yee Thane, Associate Professor, Department of Commerce, Yangon University of Economics who has provided and supervised me with her enthusiastic and valuable guidance for not only subjects of thesis paper but also the appearances.

I am very grateful to U Ba Maung Sein, Chief Operating Officer and Yoma Bank Limited for given me a chance to attend MBF Programme and for their personally assistance to get permission to be a MBF candidate. I would like to express my special thanks to respondents of Yoma Bank Limited (HO) for their helps in data collection for this study.

I would like to reveal my profound thanks and treasures to my beloved wife Ma Pwint Paing Moe for her care, understanding, and encouragement until to reach an end result of MBF degree.

Last but not the least, I would like to give my sincere appreciation to my MBF 6th Batch classmates who contribute me moral support and collaborate their encouragement to get through my study.

ABSTRACT

This study intend to analyze the compliance of the Principles for the Sound Management of Operational Risk of BCBS in Yoma Bank to have sound operational risk management framework. This study analyses with 72 emerging and noteworthy practices of 10 principles of the Sound Management of Operational Risk of BCBS. The primary data are collected by using structured questionnaire and twenty senior management level executives, such as C Level, Head of department and Deputy Head of department, were selected to answer Questionnaire during Nov and Dec 2019. This study found that, Yoma Bank need to improve in various aspect of operational risk management practices across all business and operation units to have sound Operational risk management. Especially in establishing sound operational risk management framework and robust processes to manage operational risk across business and operation units. Operational Risk Management training, including operational risk identification and assessment tools, and processes and policies, should be provided to all staff, officers, manager and above levels. Furthermore, to oversee all risks, to which a management level operational risk committee reports, operational risk committee should be formed with strong members who has vast knowledge in operational risk management. Yoma Bank is already establish Operation risk management department for building Enterprise Risk Management Framework and ERM policy. However, the whole policy procedure and practices might need to review after certain period of time based on the out coming and lesson leant during this period. Yoma Bank should perform further analysis on operation risk management frame work effectiveness with affect to financial performance of the bank.

Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

One of the key innovations associated with Basel II required banks to hold capital to deal with operation risk. The Basel Committee defined operational risk as the risk of loss due to inadequate or failed internal processes, people, and system or due to adverse external events. This type of risk exposure includes losses from employee fraud, product flaws, accounting errors, computer breakdowns, terrorism, natural disasters and fires.

Such adverse events might not only damage a financial firm's physical assets but also reduce its capacity to communicate with its customers. To get by with less capital, bankers could demonstrate to regulators they are employing effective measures to reduce operation risk, including having adequate insurance coverage, backup service capability, effective internal audits, quality contingency plans, and effective management information systems. Bank subject to Basel II were required to estimate the probability of adverse operating events and the potential losses these might generate. (Rose & Hudgins, 2013, p.503)

Due to lack of effective risk management in the system particular in the operations and its procedures, some banks have been collapsed and experienced financial problem. This issue becomes very important and gets attention after Global Financial Crisis.

Nowadays, some Myanmar banks are facing financial losses and reputational losses due to staff fraud, system failure, inadequate or failed internal processes and procedures. Central Bank of Myanmar issued several guidance that relate to Bank required to establish Operational Risk Management Framework. Implementation of sound Operational Risk Management framework will help to avoid bad reputation but also to reduce operational losses and events.

On the other hand, most of the Myanmar banks are implementing Core Banking System that enables Online and Mobile channels to the customers. The advantage of implementing Core Banking System is all the transactions can be made anywhere regardless of the location due to the centralized process. Customers can make transaction to his or her account through mobile devices or computers by using online and mobile banking. Recently, all the banks from Myanmar are transitioning to digital bank and providing financial services at any time to cater their financial needs. Therefore, the bank need to have sound operational risk management framework especially when we are transforming to digital bank due to their nature and the behavior of each customer.

Yoma Bank Limited is one of Myanmar's largest commercial banks and was established in 14 August 1993. There are only 6 branches had been opened during first four year, from 1993 to 1996. However, during 1996 and 2003, branch network are rapidly expanded up to 41 branches in 23 cities. After 2003, crisis time, there is no new branch expanding till 2010. A new chapter has begun in August, 2012 when Yoma Bank regain full banking license. As of December 2019, Yoma Bank have expanded to 80 branches in 38 cities across Myanmar.

1.1 Rationale of the study

Banking and financial sector in this country is more and more popular alongside with transformation of economy. Development and stability of Banking and financial sector become a vital role in economic development of the country. Banking and financial sector includes banks, insurance companies, credit societies, microfinance companies, fin-tech and other finance companies. Banks are the major player for the development of this sector as well as economic stability of a country. The Central Bank of Myanmar (CBM) has been liberalized and supporting banks as a regulatory body by issuing guidance and directives that the bank need to follow and implement to improve the banking and financial sector stability.

Central Bank of Myanmar (CBM) issued AML/CFT Risk Based Management Guidance Note on 27th January 2015. According to Guidance Note, Bank shall establish The Risk Management Framework encompasses with Corporate Governance, The Risk Management Function, Policies and Procedures, Internal Controls, the Compliance Function, Risk Monitoring and Reporting and Training.

CBM expects banks to establish a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduct in all aspects of their operations.

In January 2019, CBM issued directive that allow foreign banks and financial institution will be able to invest up to 35% in the equity of local banks. Before foreign banks and financial institution decide to invest to local bank, they conduct stringent due diligence process to local bank. Review on operational risk management framework of bank is one and important criteria of the due diligence checking list.

Yoma Bank, as it is a local private commercial bank, it also needs follow CBM guidelines in order to have sound, robust and effective operational risk management framework. Likewise, Yoma Banks is providing banking services to customer applying Centralized Core Banking system in brick and motor branches and with Mobile and Online channel.

In June 2019, Yoma Bank and International Finance Corporation (IFC) announced that IFC has converted loan, disbursed in 2014 to Yoma Bank, into equity to hold a 5% stake in Yoma Bank Limited. Yoma Bank can still divest another 30 % holding to foreign investor.

Based on the above discussion and highlights, this study intends to find out the operational risk management practices in Yoma Bank and to analyze the Yoma Bank's compliance of the Principles for the Sound Management of Operational Risk of Basel Committee on Banking Supervision (BCBS). A suggestion will make to provide better financial services to meet customers' requirements and its expectations with sound effective operational framework that will help the bank to success in the future.

1.2 Objectives of the study

The main objectives of the study are:

(i) To identify the operational risk management practices in Yoma Bank

(ii) To analyze the Yoma Bank's compliance of the Principles for the Sound Management of Operational Risk of BCBS.

1.3 Scope and method of the study

This study focus on over all Operational Risk Management Framework of Yoma Bank. Twenty senior management level executives, such as C Level, Head of department and Deputy Head of department, were selected to answer Questionnaire. This study aims to analyze operational risk management framework (ORMF) to prevent Operational Risk, which inherent in all banking products, activities, processes and systems.

In this study, descriptive method were used to analyze ORMF and BCBS's 11 Principle's 149 emerging and noteworthy practices, which identified when Basel Committee used to review 60 systemically important banks in 20 jurisdictions in December 2012, were used. However, this study used 72 emerging and noteworthy practices only, which compatible with and applicable with Myanmar Banking sector, as Myanmar Banking sector are still in midst of Basel I and Basel II compliance.

The questionnaire is structured with Four point Likert Scale.

I. 1 - Principle has not been implemented

II. 2 - Principle is materially not complied with

III. 3 - Principle is largely complied with

IV. 4 - Principle is fully complied with

Secondary data is gathered form respective instructions of Yoma Bank, CBM Guidelines, various level media and other relevant text and materials.

1.4 Organization of the paper

This study included five chapters. Chapter (1) is the introduction that explains rationale of the study, objectives of the study, scope and method of the study and organization of the paper. Chapter (2) shows theoretical background of the Basel II's operational risk management framework and principles for the sound management of operational risk. Chapter (3) is the profile of Yoma Bank Limited, it describes foundation of the bank, it's vision, mission, objectives, core values and motto, expansion of branches and financial services rendered by the bank within (25) years of its business life. Chapter (4) describes analysis on Operational Risk Management Framework of Yoma Bank Ltd based on the responses of (20) senior management level executives. Chapter (5) concluded with the findings and discussions, suggestions and recommendation, and need for future research to have sound Operational Risk Management Framework.

CHAPTER 2

THEORITICAL BACKGROUND

This Chapter presents the theoretical background regarding Operational Risk Management Framework. Operational risk management is quite crucial for financial institution as Operational Risk has existed for as long as financial institutions have existed. Banks are recognizing the need to more fully understand the risks of the bank's various operation activities, their interrelations within the bank and their linkage to the rest of the economy. The first section presents the definition of Operational Risk and Basel Committee on Banking Supervision's Principles for the Sound Management of Operational Risk.

2.1 Basel Committee in Banking

The Basel Committee - initially named the Committee on Banking Regulations and Supervisory Practices - was established by the central bank Governors of the Group of Ten countries at the end of 1974 in the aftermath of serious disturbances in international currency and banking markets (notably the failure of Bankhaus Herstatt in West Germany).

The Committee, headquartered at the Bank for International Settlements in Basel, was established to enhance financial stability by improving the quality of banking supervision worldwide, and to serve as a forum for regular cooperation between its member countries on banking supervisory matters. The Committee's first meeting took place in February 1975, and meetings have been held regularly three or four times a year since. (https://www.bis.org/bcbs/history.htm)

At the start of the 80s, the Basel Committee developed its very first framework for financial supervisory that came to be called BASEL I. It was majorly on capital adequacy and capital risk. The committee recommended all financial institutions to set aside 8% to fall the capital spent on loans using a single matrix system. In essence, it meant that when financial institution sanctions a loan of one hundred million, eight million should be set aside as own funds for the institution. According to Bitar et al.(2017), The paper provides substantial evidence that proves something that adherence of Basel Core principles (BCPs) has a strong positive influence on the Z-score of conventional banks, although less evident on the Z-score of Islamic banks. Using a sample of banks operating in 19 developing countries, the results appear to be driven by capital ratios, apart of Z-score for the two types of banks. Even though smaller on Islamic banks, individual chapters of BCPs also suggest appositive effect on the firm and steady nature of conventional banks. The finding support the useful role of BCP standards in improving bank strength. However, the BASELI faced a lot of critics on the ground that the system used was biased towards the financial institutions and system of the G-10 countries and was seen as narrow and incapable of guaranteeing the stability of global financial institutions. Thus leading to the development of BASELII.

Based on Basel Committee on Banking Supervision (BCBS) (2004), BASEL II depends on three reinforcement pillars in protecting financial institutions from operational risks and bring transparency in the banking sector. They include the minimum capital requirement, supervisory review process, and enhanced disclosure, Di Renzo (2007). It was BASELII that led to the explicit treatment of operational risk in financial institutions resulting in a capital measure of operational risk. According to Ibrahimovic and Franke (2017).

BASEL II is an established standard that was initially issued by the BCBS (2004). It was intended to facilitate the rules and procedures of managing operational risks in financial institutions. BASEL II requires the consideration of proper measures by financial institutions to have a culture of high-risk management across all financial institutions. Further, it reflects on the improvements of ORM practices that can assist banks and other financial institutions in planning and foresee the future. Although BASELII has been widely accepted and adopted as part of the bank practices, there are several negative opinions regarding kits applications in risk management.

Because of the negativity associated with BASEL II, in 2010, BCBS issued the third accord which was a new and a much-improved standard for the management of banks liquidity risks. BASEL III aimed at intensifying the existence of capital requirements in banks to enhance the overall strength of the global banking system. Early research on the implementation of Basel III suggests good progress. BASEL III has proved useful in providing the necessary directions for the improvement of the overall financial stability of the institutions. The primary need for Basel III was to develop a new and efficient internal control system that could be applied during the period of financial distress. However, as Basel III was an enhancement of BASEL II, it still faces many defects.

2.2 Definition of Operational Risk

There are many different ways in which operational risk can be defined. It is tempting to consider operational risk as a residual risk and define it as any risk faced by a financial institution that is not market risk or credit risk. To produce an estimate of operational risk, we could then look at the financial institution's financial statements and remove from the income statement (a) the impact of credit losses and (b) the profits or losses from market risk exposure. The variation in the resulting income would then be attributed to operational risk.

Another possible definition is that operational risk as its name implies, is the risk arising from operations. This includes the risk of mistakes in processing transactions, making payments, etc.

Some operational risks result in increases in the bank's operating cost or decreases in its revenue. Other operational risks interact with credit and market risk. (John C. Hall, 2010, p. 368)

2.3 Categorization of Operational Risks

The Basel Committee on Banking Supervision has identified seven categories of operational risk. These are:

(1) **Internal fraud:** Acts of a type intended to defraud, misappropriate property or circumvent regulations, the law, or company policy. For example, intentional misreporting of positions, employee theft and insider trading on an employee's own account.

(2) **External fraud:** Acts by third party of a type intended to defraud, misappropriate property or circumvent the law. For example, robbery, forgery, cheque kiting, and damage from computer hacking.

(3) **Employment practices and workplace safety:** Acts inconsistent with employment, health or safety laws or agreements, or which result in payment of personal injury claims, or claims relating to diversity or discrimination issues. For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability.

(4) **Clients, products and business practices:** Unintentional or negligent failure to meet a professional obligation to specific clients and the use of inappropriate

products or business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.

(5) **Damage to physical assets:** Loss or damage to physical assets from natural disasters or other events. For example, terrorism, vandalism, earthquakes, Fires and floods.

(6) **Business disruption and system failures:** Disruption of business or system failures. For example, hardware and software failures, telecommunication problems, and utility outages.

(7) **Execution, delivery and process management:** Failed transaction processing or process management,, and disputes with trade counterparties and vendors. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes. (John C Hall, 2007, P371)

2.4 The Principles for the Sound Management of Operational Risk

In June 2011 the Basel Committee on Banking Supervision published its "Principles for the Sound Management of Operational Risk" ("the Principles") to provide guidance to banks on the management of operational risk. The eleven principles incorporate the lessons from the financial crisis and the evolution of sound practice for management of operational risk. The Principles cover governance, the risk management environment and the role of disclosure, and address the three lines of defence (business line management, an independent corporate operational risk management function and an independent review). (BCBS 292, 2014)

Principle 1: Operational risk culture

The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation. (BCBS 292, 2014)

Principle 2: Operational risk management framework

Banks should develop, implement and maintain a framework that is fully integrated into the bank's overall risk management processes. The framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Principle 3: Board of directors

The board of directors should establish, approve and periodically review the framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: Operational risk appetite and tolerance

The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume. (BCBS 292, 2014)

Principle 5: Senior management

Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance. (BCBS 292, 2014)

Principle 6: Risk identification and assessment

Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. (BCBS 292, 2014)

Principle 7: Change management

Senior management should ensure that there is an approval process that fully assesses operational risk for all new products, activities, processes and systems. (BCBS 292, 2014)

Principle 8: Monitoring and reporting

Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms that support proactive management of operational risk should be in place at the board, senior management, and business line levels. (BCBS 292, 2014)

Principle 9: Control and mitigation

Banks should have a strong control environment that utilises policies, processes and systems, appropriate internal controls, and appropriate risk mitigation and/or transfer strategies. (BCBS 292, 2014)

Principle 10: Business resilience and continuity

Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption. (BCBS 292, 2014)

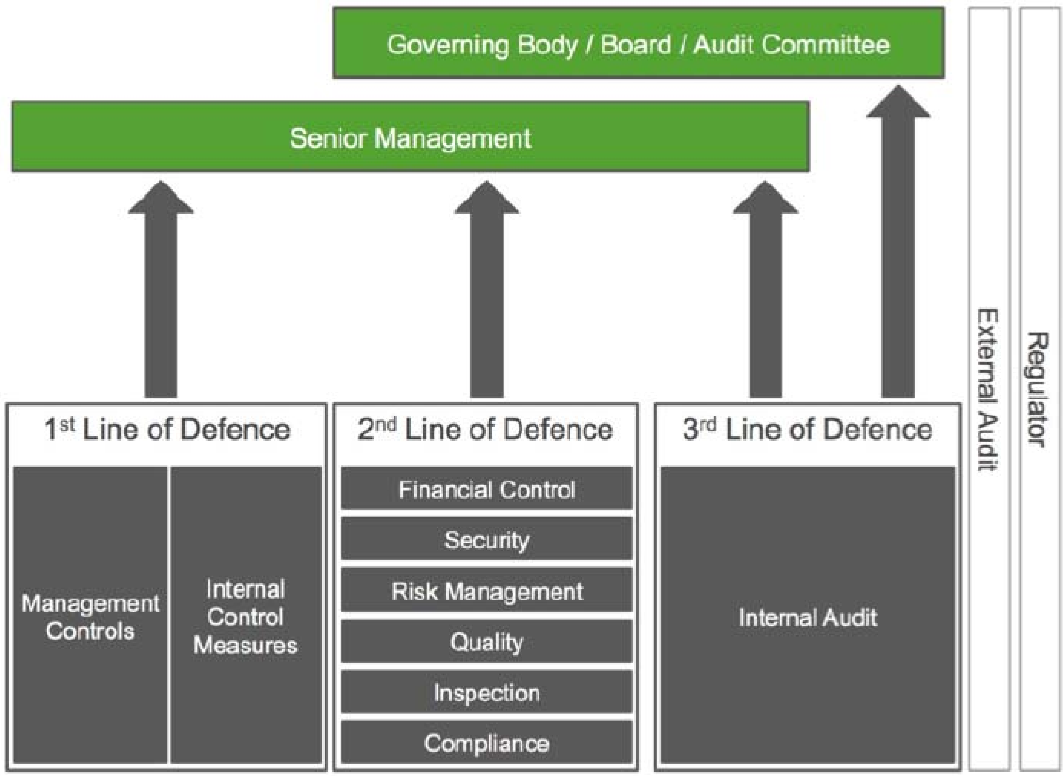
Principle 11: Role of disclosure

A bank's public disclosures should allow stakeholders to assess its approach to operational risk management. (BCBS 292, 2014)

2.5 Operational Risk Management Framework

To identify, assess, monitor and report the risks to which an organisation may be exposed currently or potentially is the key objective of Operational Risk Management Framework. The framework should be cohesive, consistently applied and integrated with business processes necessarily.

Figure (2.1) Operational Risk Management Framework



Source: Anderson and Eubanks (2015)

There are 7 key components included in Operational Risk Management Framework as follow,

(1) First line of defence

First line of defence responsibilities include using operational risk management tools to identify and manage risks, assessing and enhancing controls, monitoring and reporting the operational risk profile, ensuring that the operational risk profile adheres to the established risk appetite and tolerance, complying with policies, standards and guidelines, and promoting a strong risk culture. (BCBS 292, 2014, P34)

(2) Second line of defence

Second line of defence responsibilities include designing operational risk management tools used by the business to identify and manage risks, applying "independent challenge" to the use and output of the operational risk management tools by the first line of defence, developing and maintaining policies, standards and guidelines, reviewing and contributing to the monitoring and reporting of the operational risk profile, designing and providing operational risk training and awareness, and promoting a strong risk culture.

(3) Third line of defence

Third line of defence responsibilities include independently verifying that the ORMF has been sufficiently well designed and implemented by both the first and second lines of defence, reviewing the "independent challenge" applied by the second line of defence to the first line of defence's use and output of the operational risk management tools, reviewing the monitoring, reporting and governance processes, and promoting a strong risk culture.

(4) The Board

The board has ultimate responsibility for the bank's business strategy and financial soundness, key personnel decisions, internal organisation and governance structure and practices, and risk management and compliance obligations. (BCBS 294, 2015, P 7)

(5) Senior Management

Senior management consists of a core group of individuals who are responsible and accountable to the board for effectively overseeing the day-to-day management of the bank. (BCBS 294, 2015, P 18)

(6) External Audit

An external auditor conducts the audit of a bank's financial statements to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, thereby enabling the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework, and to report on the financial statements, and communicate as required by internationally accepted auditing standards, in accordance with the auditor's findings.

External auditors play a vital role in maintaining market confidence in audited financial statements. In the case of the banking industry, this public role is particularly relevant to financial stability given banks' financial intermediation function within the economy as a whole. Audit quality is key to the effectiveness of such public role. In addition, the external auditor has a duty to report directly to the supervisor (or, where not permitted, indirectly through the bank) on matters of material significance arising from the audit of the bank. (BCBS 280, 2014, P 2)

(7) **Regulator**

The Central Bank of Myanmar (Regulator) ensures prudent practices at the individual bank level, through the imposition of capital standards and operational guidelines and also reducing systemic risk, through regular auditing, examination and risk based supervision.

2.6 Literature Review

The Basel Committee on Banking Supervision published "Principles for the Sound Management of Operational Risk" in June 2011 in order to provide guidance to banks on the management of operational risk.

Operational risk is the vast discipline focusing on the risks increasing from the people, systems, and processes through which a firm operates. It can also include other Categories of risk, such as legal risk, fraud, physical or environmental risks. Revell (1979). It arises from a wide range of activities like acts of frauds, errors, negligence, violations, events of technological failures, process deficiencies, systems flaws, actions of terrorists and vandalism, natural disasters, like floods, earthquakes, etc, Hussain et al. (2014).

In December 2012, the BCBS's Working Group on Operational Risk (WGOR) performed the review of the implementation of the Principles. Conducted via a questionnaire, the review aimed to:

- identify and understand the degree to which banks have implemented the Principles;
- identify common significant gaps at banks related to the implementation of the Principles; and
- identify emerging and noteworthy practices in operational risk management that are used by banks but which are not currently addressed by the Principles.

A questionnaire was used to solicit self-assessments from participating banks. There are 180 questions contained in the questionnaire and 60 systemically important banks across 20 jurisdictions were completed the questionnaire. The questionnaire covered all 11 Principles as well as the on the overarching guidance related to the three lines of defence.

Banks were asked to self-assess and rate their operational risk management practices on a rating scale of “1” to “4” or “N/A". The four ratings were defined as follows:

1 - Principle has not been implemented

2 - Principle is materially not complied with

3 - Principle is largely complied with

4 - Principle is fully complied with

In 6th October 2014, The Basel Committee on Banking Supervision published Review of the Principles for the Sound Management of Operational Risk, BCBS 292.

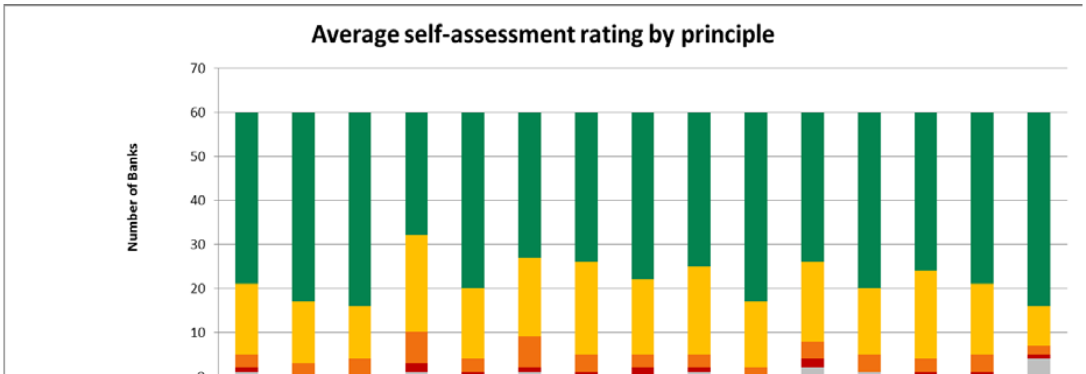
Key findings and observations from this review are as follow,

Overall, banks have made insufficient progress in implementing the Principles originally introduced in 2003 and revised in 2011. Many banks are still in the process of implementing various principles. Systemically important banks (SIBs) have implemented the Principles and the operational risk management tools to varying degrees. Historically, implementation of the Principles was strongly aligned with the Basel Framework’s approaches to calculating operational risk capital requirements such as The Standardised Approach (TSA) and the Advanced Measurement Approach (AMA). Banks applying these more advanced approaches are expected to have more advanced operational risk management frameworks and implement to a greater degree the operational risk management tools, which include risk and control self-assessments (RCSAs), internal loss data collection, scenario analysis, external data collection and analysis, key risk indicators (KRIs)/key performance indicators (KPIs), change management and comparative analysis.

Some SIBs, however, have yet to implement all of the Principles and do not deploy the full range of operational risk management tools. This may be because some of the banks are not subject to the most advanced approaches to operational risk and the associated higher expectations for managing the risk. Therefore, these banks may not be adequately identifying and managing their operational risk exposures. Methods for identifying and managing operational risk should be seen as complementary to the calculation of operational risk capital requirements, rather than as a consequence of that activity. Aligning the implementation of the risk management principles with the risk profile and systemic importance of banks, rather than the approaches selected to calculate operational risk capital requirements, is also be consistent with the objective of more intensive and effective supervision of systemically important banks.

The following chart summarises the average bank ratings 4,5 for each of the Principles and the three lines of defence.

Figure (2.2) Average self-assessment rating by principle



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	3 LOD	1st LOD	2nd LOD	3rd LOD
Fully complied with	39	43	44	28	40	33	34	38	35	43	34	40	36	39	44
Largely complied with	16	14	12	22	16	18	21	17	20	15	18	15	20	16	9
Materially not complied with	3	3	4	7	3	7	4	3	3	2	4	4	3	4	2
Not been implemented	1	0	0	2	1	1	1	2	1	0	2	0	1	1	1
Not applicable	1	0	0	1	0	1	0	0	1	0	2	1	0	0	4
Average	3.50	3.64	3.65	3.25	3.59	3.32	3.45	3.54	3.50	3.68	3.37	3.52	3.55	3.56	3.47

Source: BCBS 292, 2014, P 2

This review has identified various challenges and themes within each of the principles. Four principles have been identified as among the least thoroughly implemented by banks including (i) operational risk identification and assessment, (ii) change management, (iii) operational risk appetite and tolerance, and (iv) disclosure. In addition, weaknesses have been observed in the implementation of the overarching principle of the three lines of defence. (BCBS 292, 2014, P 1)

Based on "Review of the Principles for the Sound Management of Operational Risk", 72 emerging and noteworthy practices of 10 principles were used to analyse Yoma Bank's compliance to the Principles for the Sound Management of Operational Risk of BCBS.

CHAPTER 3

BACKGROUND STUDY OF YOMA BANK LIMITED

This chapter highlights the General situation of Myanmar banking industry and the profile and Operational risk management practices of Yoma Bank Limited, it describes foundation of the bank, it's vision, mission, objectives, core values and motto, expansion of branches and financial services rendered by the bank within (26) years of its business life.

3.1 Overview of Banking Industry of Myanmar

Myanmar has changed its 26 years old, centrally planned economic system into the market oriented economic system in the late 1988. The new Government, the State Law and Order Restoration Council enacted the new banking laws, the Central Bank of Myanmar law, the Financial Institution of Myanmar Law, the Myanmar Agricultural and Rural Development Bank Law and the New Saving Bank Law in 1990 and 1992.

The Central Bank of Myanmar (CBM) has already granted banking license to (27) domestic private banks to operate as commercial banks or development banks. Also, CBM issued Banking license to 13 Foreign Bank to open branches and (5) Mobile financial institutions including Digital Money Myanmar (Brand Name: Wave Money) which is jointly own by Yoma Bank Limited, Telenor Myanmar Limited and First Myanmar Investment Co Ltd. The lists of those financial institutions are shown in Appendix A, B and C.

In Myanmar most of domestic private banks faced with banking crisis in 2nd week of February, 2003. At that time, the Central Bank of Myanmar (CBM) intervened by imposing restrictions on withdrawals of deposits and giving instructions to the private banks to recall loans. Because of the banking crisis, the Banking Supervision Committee closely monitors the daily operations of some private banks to perform normal banking functions with some limitations. Therefore both deposits and loans of private banks increased and gradually recovered to the positions of before banking crisis.

The Financial Institutions of Myanmar Law (FIML) (1990) allows the private sector to operate the domestic commercial banking, the investment of development banking, the finance companies and the credit societies with the approval of the Central Bank of Myanmar. In 25th Jan 2016, Pyidaungsu Hluttaw enacted New Financial Institutions of Myanmar Law (2016) which supersede old FIML (1990).

Compared with the old FIML (1990), the new FIML (2016) comprehends detail guidelines for both foreign and domestic financial institutions, covering all essential areas such as responsibilities, powers and objectives of the supervisory authority, and prudential regulations and requirements for all financial institutions.

Although the 1990 law facilitated private participation in the banking sector, the new FIML (2016) is deliberated to cover detailed corrective action and Bank resolution measures for insolvent banks including appointment of administrator and rehabilitation programs for the failing bank. The new FIML (2016) encourages transparency, accountability and good corporate governance in the system. It is a comprehensive framework for effective implementation of a stable and modern banking system which would be able to support the economy to achieve a sustainable development.

As clearly stated in the CBM's FY 2018 Transaction Period Report (April to September), Part III, section 3.20 and 3.21. CBM's the main objectives of on-site supervision are as follows:

a) To ensure the health of the banking sector,

b) To monitor the performance of individual banks and their position in the banking system,

c) To identify problems for taking corrective measures action in time,

d) To minimize risks.

Central Bank of Myanmar has received Technical Assistance from IMF since 2018 for adopting Risk-based supervision from Compliance-based Supervision. After that Financial Institutions Supervision Department issued internal guideline and user manual and testing to some banks by Risk-based Supervision while performing Compliance-based Supervision. Central Bank of Myanmar has a plan to fully adopt Risk-based Supervision in 2020.

New practice of Risk Base Supervision will be focused on identifying the risk profiles of banks. These risks include level of Credit Risk, Market Risk, Liquidity Risk, Operational Risk, Legal/Regulatory and Reputational Risk, Strategic risk, Group risk.

Monitoring Key Financial Ratios with forward looking assessments and closely overseeing how the emerging risks are mitigated by Management and Board by using Internal Control Questionnaires (ICQs) of Qualitative Assessment and Quantitative Analysis. Besides, all banks require preparing a greater focus on risks to control the acceptable low level and understanding of the financial system's development in line with the changing of Macroeconomic environments. (FY 2018 Transaction Period Report (April to September), P 80)

3.2 Brief Description of the Yoma Bank Ltd

Yoma Bank Limited is one of Myanmar's largest commercial banks. It was established in 14 August 1993; with its first branch is Yangon Main branch in Mingalartaungnyunt Township, Yangon. There are only 6 branches had been opened between 1993 and 1996. However, during 1996 and 2003, branch network are rapidly expanded to 41 branches in 23 cities.

Yoma Bank was among many privately owned banks affected in the 2003 banking crisis, during which consumer confidence dropped after rumors spread throughout the country about the security of savings accounts. Like most all other privately owned banks in the country, the bank was solvent and maintained a sound loan to equity ratio, but was unable to withstand the abrupt and massive withdrawal of deposits and had to resort to the Central Bank's support. Yoma Bank's operations were subsequently curtailed and were allowed to remain open with only remittance services.

Despite being restricted to provide domestic remittances services only, Yoma Bank maintained profitability. Large number of branches throughout the country coupled with efficient service has enabled Yoma Bank to maintain a significant market share. To this day Yoma Bank's remittance service remains the most trusted in the country.

On the 23rd of August 2012, Yoma Bank finally regained permission to operate under a full banking license. Nowadays, Yoma Bank has 80 branches throughout the country and has to provide more services and expand branch network in strategically important town in the whole country.

3.3 Core Values and Motto

Yoma Bank Limited always tries to serve its customers in the best ways for their satisfaction. It also values all employees in the organization. Yoma Bank Limited has developed a statement of core values to guide the bank's pursuit of its vision, mission, objectives and ways of day to day operations and the behavior of the bank personnel.

The bank's core values are:

- Innovation
- Integrity
- Respect
- Teamwork
- Customer

The bank's motto is "Yoma Bank, The Responsible Bank". Yoma Bank Limited believes that the customers are the reason they exist in the industry.

3.4 Financial Services rendered by Yoma Bank Ltd

Yoma Bank Limited gradually extended its financial institutions to meet its customers' requirements. At the first fiscal year of 1993-94 of its establishments, Yoma Bank Limited served its customers with checking accounts (Current accounts), Saving accounts, Time deposit or fixed deposit accounts for depositors. Many customers were satisfied on Yoma Bank's services for checking privileges in checking accounts, earning interest in saving deposit accounts and fixed deposit accounts.

Yoma Bank Limited also disbursed loans and advances at the first year of its establishment in 1993. Providing professional and seamless services to its customers has been the most important goal for Yoma Bank Limited. The management and employees of the bank always endeavor to provide the desirable financial services to their customers. Yoma Bank Limited is the first bank in the country which offered hire-purchase for a wide range of consumer goods. Hire-purchase is the installment credits to customers to support the purchases of durable such as automobiles, motor cycles, refrigerators, washing machines, copying-machines, computer hardware and so on.

At the second year of its establishment, in 1994-95 fiscal years, Yoma Bank Limited launched its own credit card, the "YOMA CARD" first in the country. It offered its cardholders a convenience for payments of goods and services instead of handling cash. The immediate and wide acceptance of the YOMA CARD amongst merchants and cardholders indicated that it was a vast potential and substantiates the bank's belief that such a service was much needed in the society at that time. Because of the YOMA CARD continues to receive wide acceptance in the Yangon market, it expanded its markets and geographic acceptance to Mandalay market in the 1995-96 fiscal year. Yoma Bank Limited introduced its customers a new service of flexibility in their current and savings accounts. It was an automatic transfer of funds between checking accounts (current accounts) and saving accounts, it was also called cross-reference system.

Yoma Bank Limited started its internal remittance service at the beginning of the 1995-96 fiscal years between Yangon and Mandalay by using fax machines. Yoma Bank Limited continues to introduce new financial instruments and innovative services to serve its customers. In the fiscal year 1997-98, the bank launched the Yoma Gift Cheque an attractive and most appropriate present applicable to almost all auspicious occasion's year around. Yoma Bank Limited embarked upon an ambitions modernization program to fully computerize its operations. A brand new fully computerized banking operation, Yoma Integrated Banking System (YIBS) was successfully started in 2000-01 financial year as an efficient banking operation for bank and its customers.

A significant event in the fiscal year 2001-02 was the implementation of satellite communications for banking network of all (41) branches of Yoma Bank Limited. With the introduction of this highly efficient communications and data transmission system, the bank has been also able to provide much more innovative services to all its customers and continue to hold its competitive edge in the local banking community.

In July 2016, Yoma Bank Limited start migrated banking operation from YIBS to Fusion Banking Essence (FBE) Core Banking System developed by Misys (Finastra). In Jan 2018, all Yoma Bank branches migrated to Fusion Banking Essence (FBE) Core Banking System.

In 2016, Yoma Bank, together with Telenor Southeast Asia Investment Pte Limited, Telenor Go Pte Limited & Telenor Global Services Singapore Pte Limited, founded Wave Money, Myanmar's first mobile financial service and now the largest mobile money platform in the country (FMI Annual Report, 2017-2018).

In 2017, Yoma Bank launches its SMART digital account and new mobile banking App and online banking platform continuing to lead the way in modern, world-class banking.

Yoma Bank Limited also provided other subsidiary banking services such as receiving safe custody of securities, documents and valuables, collecting drafts and cheques for its customers, and issuing various guarantees: tender guarantee, repayment guarantee or advance payment guarantee, performance guarantee and trade guarantees.

At the present, Yoma Bank Limited more emphasizes on getting deposit and issue loans and advances to Corporate Customers, SME customers and Retailed customers than internal remittances service. Yoma Bank Limited is a first runner in Home Loan product and Price Linked Account (JZu). Major financial services provided by Yoma Bank Limited are shown in Table 3.1.

Table 3.1. Major financial services provided by Yoma Bank Limited

Sr. No.	***Financial Services***
1.	Accepting Saving Accounts
2.	Accepting Current Accounts
3.	Accepting Fixed Deposits Accounts
4.	Issuing Payment Orders
5.	Internal Remittance
6.	Loans and Overdrafts
7.	Issuing Bank Guarantees
8.	Safe Deposit Locker
9.	Foreign Currency Exchange Counter
10	International Banking
11	Trade Finance
12	Home Loan
13	Trade Guarantees
14	Hire-Purchase

Source: Yoma Bank Ltd

3.5 The Operational Risk Management practices of Yoma Bank Limited

Yoma Bank established Corporate Governance structure since 2013, corporate governance policy properly enacted in October 2015. There are two major board committees under Board of Directors as follow,

1. Audit Committee
2. Risk Oversight Committee

Management committee directly reports to the board. There are four major committees under Management Committee as follow,

1. Credit Committee
2. Asset Liability Committee
3. Product committee
4. NPL Committee

Board of Director also established a code of conduct that sets clear expectations for integrity and ethical values of the highest standard and identifies acceptable business practices and prohibited conflicts. Following are Code of conduct of Yoma Bank,

1. Act with integrity and honesty
2. Avoid conflicts of interest
3. Avoid related party transactions
4. Refuse gifts
5. Do not become involved with bribery or corruption
6. Act responsibly and follow rules and legislation
7. Report misconduct

Although Yoma Bank not yet properly established Operational Risk Management Framework, Yoma Bank establish Operational risk mitigating practices across the operating environment of products and services delivered. For instance, in Foreign Exchange (FX) dealing, Treasury front office team deals with customer, Treasury operation team make transaction for fund settlement. By doing so, Foreign Exchange (FX) dealing transaction cannot be done by one department, section or person.

Likewise, every commercial loan originating come through Yoma Bank branches and Corporate Banking department, however, each loan was processed by Credit risk department and credit decision were made by Credit Committee, finally, loan disbursement was done by Credit Administration Department.

Yoma Bank's internal audit department conduct regular auditing activities not only to branches but also to head office departments. When internal audit team visit to branches and departments, they perform detailed end-to-end analysis of branch/department's daily operation and compliance measure of SOPs.

Yoma Bank establish Core Operation Department to monitor issues and mistake, which came out from day to day operation activities and system activities, such as interest rate change, fees waivers, journal entries and some daily closing reports. By doing so, some operational risk items are being removed or mitigated.

To have clear segregation of duties (SODs), relates to specific products and services, among department and section to get better control environment, Yoma Bank review and update Standard operation procedures (SOPs), Service Level Agreements (SLAs) regularly.

Yoma Bank start establish Operational Risk Department in Oct 2019 by getting technology and knowledge assistant by Rabo Bank, 110 year old bank from Netherlands, to implement Enterprise Risk Management and Operation Risk Management.

CHAPTER 4

ANALYSIS ON THE COMPLIANCE OF THE PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK IN YOMA BANK

This chapter analyse the compliance of the Principles for the Sound Management of Operational Risk in Yoma Bank Limited is mainly based on the primary data collected through systematically developed by 4 point Likert scale questionnaire. A sample of 20 respondents was conveniently selected from senior management level executives, such as Chief Officer Level (COO, CRO, and CPO etc.), Head of department and Deputy Head of department and all respondents responded to the questionnaires.

4.1 Research Design

The questionnaire is developed to explore the demographic factors of the respondent, and the assessment of compliance of the Principles for the Sound Management of Operational Risk in Yoma Bank Limited. Although, there are eleven principles in The Principles for the Sound Management of Operational Risk (BCBS 292, 2014), some principles and emerging and noteworthy practices are not applicable in Myanmar, thus, emerging and noteworthy practices' 72 criteria of 10 principles were used in questionnaire.

The questionnaire is divided into 3 parts with 72 attributes. They are: guidance for questionnaire ratings, respondents' demographic information and assessment of the ORMF with Emerging and noteworthy practices.

4.2 Profile of Respondent

The profile of respondents include age, gender, education level and year in banking and finance industry intend to get level knowledge of respondents on operational risk management practices.

Respondents by age Group

Respondents' perception and attitude depend on their age levels. There are five levels of age groups:

1. Between 30 and 35
2. Between 35 and 40
3. Between 40 and 50
4. Between 50 and 60
5. 60 and above.

It is found that among 20 respondents, most of them are age between 41 and 50 years and it represents 60%. Second largest age group is between 36 and 40 years and it hold 25%, then 15% between 51 and 60 years. The analysis of age level is shown in table 4.2.

Table (4.2) Number of respondents by age group

Sr No	***Age Group***	***Frequency***	***Percent***
1	30-35 years	-	-
2	36-40 years	5	25
3	41-50 years	12	60
4	51-60 years	3	15
5	61 years and above	-	-
Total		20	100

Source: Survey data (2019)

As a result the majority of respondents who answered survey questionnaire are mature levels of age for analyzing Operational Risk Management practices of Yoma Bank Limited.

In addition, this mature level of age group has ability to evaluate Operational Risk Management practices of Yoma Bank Limited.

Respondents by Gender

The composition of gender (male and female) in the sample is shown in Table 4.3. According to Table 4.3, the majority of all respondents are male and they share 70% of the sample while female respondents are 30% of the sample.

Table (4.3) Number of respondents by gender

Sr No	Gender	Frequency	Percent
1	Male	14	70
2	Female	6	30
Total		20	100

Source: Survey data (2019)

Respondents' service year in Banking and Finance industry

The respondents were asked about their service year in banking and finance industry. The service year are classified into four group: under 5 year, 5 to 10 year, 10 to 20 year and above 20 years. The results are shown in Table 4.4.

Table (4.4) Number of respondents by service year in Banking and Finance industry

Sr No	Service year in Banking and Finance industry	Frequency	Percent
1	Under Five Year	-	-
2	5-10 Year	4	20
3	11-20 Year	11	55
4	above 20 Year	5	25
Total		20	100

Source: Survey data (2019)

The level of service year may support in evaluation of Operational Risk Management practices of Yoma Bank Limited. The higher the service year level the higher the level of assessment to Operational Risk Management practices of Yoma Bank Limited.

Respondents by Education Level

The respondents were asked about their education level. The education levels of respondents are classified into five groups; high school level, bachelor degree, master degree, Ph.D., and other such as medical doctors and engineers. The results of the survey state that 50% of respondents are bachelor degree holders, 5% high school level. 35% master degree holders and 10% Ph.D., holders. The results state that almost all the respondents are graduated persons. The results are shown in Table 4.5.

Table (4.5) Number of Respondents by Education Level

Sr No	***Education Level***	***Frequency***	***Percent***
1	High School	1	5
2	Bachelor	10	50
3	Master degree	7	35
4	Ph.D.	2	10
5	Others	-	-
Total		20	100

Source: Survey data (2019)

The level of education may support in evaluation of Operational Risk Management practices of Yoma Bank Limited. The higher the educations level the higher the level of assessment to Operational Risk Management practices of Yoma Bank Limited.

4.3 Assessment of the ORMF of Yoma Bank

In this section, assessment of the Yoma Bank's operational risk management practices with emerging and noteworthy practices, which contains 108 criteria of 10 principles to identify compliance to the Principles for the Sound Management of Operational Risk (BCBS 292, 2014)

Table (4.1) Guidance for Questionnaire Ratings

Rating	Description
4 – Principle is fully complied with	The bank is entirely compliant with the principle, there is evidence to substantiate the assessment, and there are no outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties
3 – Principle is largely complied with	The bank is non-compliant in only minor aspects of the principle, the non-compliance is not deemed to be material overall and there may be some minor outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
2 – Principle is materially not complied with	The bank is non-compliant in major aspects of the principle, and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
1 – Principle has not been implemented	The bank is entirely non-compliant with the principle and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
0 – Not applicable	The Principle is not yet applicable to the bank.

Source: BCBS 292, 2014

Principles 1: Operational Risk Culture

The respondents were asked to rate and describe to what extent of the operational risk culture had been implemented in Yoma Bank. The respondents' perception on principle (1) Operational risk culture's emerging and noteworthy practices of Yoma Bank is shown in Table (4.6).

Table (4.6) Principles (1) Operational Risk Culture

Sr No	Practices No	Emerging and noteworthy practices	Mean
1	R1	The code of conduct applies to all the bank's staff and appointees, including members of the board of directors.	3.05
2	R2	The code of conduct or ethics policy is regularly reviewed and attested to by employees, is regularly approved by the board of directors, and is publicly available on the bank's website.	2.05
3	R3	Establishment and implementation of a whistle-blower programme.	2.55
4	R4	Linking the compensation programme and remuneration to risk-adjusted indicators.	1.8
5	R5	Establishing operational risk awareness for all employees; more advanced training on the operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities.	1.25
6	R6	Customised and mandatory operational risk training for many roles including business unit operations, supervisory levels, senior management, and the board of directors.	1
Average			1.95

Source: Survey data (2019)

As described in the table 4.6, R1 mean score is 3.05, As Yoma Bank has implemented Code of Conduct and all respondents are aware of this Code of Conducts. Besides, Yoma Bank should enhance to have clear expectations for integrity and ethical values of the highest standard. Also, Yoma Bank should identifies business practices and conflicts to compliance with all applicable laws, rules and regulations.

However, as R2 mean score is 2.05, it can be conclude that Yoma Bank is not regularly review the code of conduct and attested to by employees. Also, Yoma Bank should regularly review the code of conduct and get approved by the board of directors. Moreover, Code of conduct should be available on the Yoma Bank's website.

Likewise, R3 mean score is 2.55, it can be conclude that, Yoma Bank has established whistle-blower programme as Yoma Bank create Email address that everyone can report or raised issues, misappropriate action.

R4 mean score is 1.8, it can be conclude that, Yoma Bank has not established compensation programme and remuneration that balance risk and reward.

R5 and R6 are relate to risk management training, mean score are 1.25 and 1 respectively, it can be conclude that Yoma Bank is not providing proper training to all employees. Yoma Bank should provide proper Risk Management training regarding operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities.

Principles 2: Operational Risk Management Framework

The respondents were asked to rate and describe Yoma Bank's current degree of implementation for many aspects related to their operational risk management framework (ORMF). The respondents' perception on principle (2) Operational risk management framework's emerging and noteworthy practices of Yoma Bank is shown in Table (4.7).

Table (4.7) Principles 2: Operational Risk Management Framework

Sr No	Practices No	Emerging and noteworthy practices	Mean
7	R7	The ORMF was reviewed and updated to ensure alignment following the publication of the enhanced BCBS Principles for the Sound Management of Operational Risk in June 2011.	0.45
8	R8	Referencing the relevant operational risk management policies and procedures.	1.25
9	R9	Applying the ORMF to all the bank's material operating groups and entities, including subsidiaries, joint ventures and geographic regions.	0.45
10	R10	The ORMF requires consistent implementation of the bank's operational risk taxonomy across all business lines and operational risk tools.	0.45
11	R11	Describing the roles and responsibilities of each of the three lines of defence as they relate to the use of the operational risk identification and assessment tools.	1.75

12	R12	Establishing the mandates, membership, and representation of various operational risk governance committees.	1
13	R13	Establishing a quality assurance programme to ensure that independent challenge and review, as applied by the second line of defence, results in consistent risk and control assessments.	0.9
14	R14	Creation of an operational risk dictionary that includes definitions and examples of the various operational risks in the bank's taxonomy. In addition, the dictionary includes guidance related to the classification of each of the operational risks within the taxonomy, to ensure consistent identification and classification across the bank.	0.2
15	R15	Establishing a control library to inventory all the controls within the bank and each of its business lines.	0.75
16	R16	Defining operational risk events beyond direct financial losses, so that such events include indirect losses such as forgone revenue and lost business, and reputational damage.	0.95
Average			0.82

Source: Survey data (2019)

As described in the table 4.7, all R7, R8, R9, R10, R11, R12, R13, R14, R15 and R16 got mean score under 1, it can be conclude that Yoma Bank not yet established Operational risk management framework that comply with the The Principles of BCBS. Although Yoma Bank has established Operational risk management practices in some area of day to day operation, such as having proper SOPs, SLA and SODs for products and services and End of Day checking procedures that mitigate branches' day to day operation risk. However, Yoma Bank should establish proper operational risk management framework, that clearly articulate operational risk management policies and procedures, implementation of the bank's operational risk taxonomy across all business lines and operational risk tools and Establishing a quality assurance programme to ensure that independent challenge and review, as applied by the second line of defence, results in consistent risk and control assessments.

Principle 3: Board of Directors

The respondents were asked to rate and describe Yoma Bank's current degree of implementation for a variety of board-related elements. The respondents' perception on principle (3) Board of directors' emerging and noteworthy practices of Yoma Bank is shown in Table (4.8).

Table (4.8) Principles 3: Board of Directors

Sr No	Practices No	Emerging and noteworthy practices	Mean
17	R17	Establishing a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identifies acceptable business practices and prohibited conflicts.	2.8
18	R18	The board regularly challenges senior management on the design and effectiveness of the bank's operational risk management framework.	2.3
19	R19	The board reviews and approves an operational risk strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation.	1.7
20	R20	The board supports the establishment of a formal culture communications strategy, whereby senior management communicates the importance of strong risk management practices through a variety of forums such as employee communications and formal training sessions.	2.35
21	R21	The board ensures that internal audit includes the ORMF as a focus within business unit audits, to complement the overall audit of the ORMF.	2.25
22	R22	The board ensures that the scope of internal audit's work on the bank's ORMF is not limited to risk measurement (ie model) activities and includes a sufficient focus on risk management activities.	2
Average			2.23

Source: Survey data (2019)

As described in the table 4.8, all R17, R18, R20, R21 and R22 got mean score 2.8, 2.3, 2.35, 2.25 and 2 respectively. It can be conclude that Yoma Bank has strong corporate governance and Board of director oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels. As there are two major board committees under Board of Directors, Audit committee and Risk Oversight Committee, the board of directors ensures that the scope of internal audit's work on the bank's ORMF is not limited to risk measurement (ie model) activities and includes a sufficient focus on risk management activities. However, R19's mean score is 1.7, it can be conclude that, board of directors are not reviewing and approve operational risk strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation.

Principle 4: Operational Risk Appetite and Tolerance

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to operational risk appetite and tolerance. The respondents' perception on principle: 3 Operational risk appetite and tolerance's emerging and noteworthy practices of Yoma Bank is shown in Table (4.9).

Table (4.9) Principles 4: Operational Risk Appetite and Tolerance

Sr No	Practices No	**Emerging and noteworthy practices**	Mean
23	R23	Defining operational risk appetite and tolerance at both a divisional and taxonomy level.	1.25
24	R24	Utilising both quantitative and qualitative components within the bank's operational risk appetite and tolerance statement.	1.25
25	R25	Setting limits based on established key risk indicators such as loss metrics, deficiencies, events and residual risk assessments using operational risk identification and assessment tools that have been implemented.	1
Average			1.17

Source: Survey data (2019)

As described in the table 4.9, all R23, R24, and R25 got mean score 1.25, 1.25 and 1 respectively. It can be conclude that Yoma Bank's board of directors are not approving and reviewing the risk appetite and tolerance statement that capture the various operational risk appetites within a Yoma Bank and ensure that they are consistent. The aptness of limits and the overall operational risk appetite and tolerance should be reviewed by board of directors regularly to the extent of changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches.

Principle 5: Senior Management

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to senior management. The respondents' perception on principle: 5 Senior management's emerging and noteworthy practices of Yoma Bank is shown in Table (4.10).

Table (4.10) Principles 5: Senior Management

Sr No	Practices No	**Emerging and noteworthy practices**	Mean
26	R26	Ensuring that an appropriate level of operational risk training is available at all levels throughout the organisation and that the training reflects the seniority, role and responsibility of the individuals for whom it is intended.	1
27	R27	Membership of the operational risk committee consists of the first line of defence, the CORF, and other second line of defence control functions.	0.95
28	R28	ORC meetings are convened regularly, minutes are prepared, and action items are tracked to completion.	0.7
29	R29	Succession plans for key operational risk individuals have been established to ensure continuation of critical operations and maintenance of expertise.	1.2
Average			0.96

Source: Survey data (2019)

As described in the table 4.10, all R26, R27, R28 and R29 got mean score 1, 0.95 0.7 and 1.2 respectively. It can be conclude that Yoma Bank's senior management not yet established and support appropriate operational risk governance structure, line of responsibility, sufficient corporate operational risk function (CORF) stature and operational risk committee. Yoma Bank should establish operational risk committee, to oversee all risks, to which a management level operational risk committee reports, with members who have expertise in banking business activities and financial as well as independent risk management.

Principle 6: Risk Identification and Assessment

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to risk identification and assessment. The respondents' perception on principle: 6 Risk identification's emerging and noteworthy practices of Yoma Bank is shown in Table (4.11).

Table (4.11) Principles 6: Risk Identification and Assessment

Sr No	Practices No	Emerging and noteworthy practices	Mean
30	R30	The consideration of internal audit findings as an input to the various operational risk management tools (eg RCSAs, scenarios, key risk/performance indicators etc).	2.55
31	R31	The bank employs a process that considers audit findings in the challenging of business self-assessments.	2.8
32	R32	The bank's audit function conducts a detailed end-to-end analysis of the operational risk profile assessment process, including assessments of process governance, the detail and quality of reporting, the process by which deficiencies are identified, tracked, and remediated, and generally whether the programme is functioning in a manner consistent with established policies.	2
33	R33	The use of internal audit findings to compare management's risk and control assessments with the various operational risk management tools.	2.25
34	R34	The use of internal audit findings as an input to the regular updating of the bank's operational risk profile.	2.25

35	R35	Monitoring the number of open and overdue internal audit issues as a key indicator.	3.05
36	R36	Implementing a business process framework that provides guidelines for the creation of business process maps.	2.55
37	R37	Undertaking a risk-based approach to business mapping, implying a focus on high-risk processes rather than all business processes within the bank.	2.55
38	R38	Establishing a central repository for all business process maps.	2
39	R39	Embedding the bank's operational risk taxonomy into the business process mapping methodology for aggregation and comparison with the operational risk profile.	2
40	R40	Establishing key risk and performance indicators at multiple levels throughout the bank, including at the group-wide level, the divisional level, and the individual business-line level.	2.05
41	R41	KRIs, KPIs and escalation triggers are subject to regular review and enhancement.	1.75
42	R42	The first line of defence creates action plans for metrics that breach their respective thresholds.	2
43	R43	The second line of defence independently challenges the selection of indicators and thresholds, as well as the proposed action plans.	2
Average			2.27

Source: Survey data (2019)

As described in the table 4.11, all R30, R31, R33, R34 and R35 got mean score 2.55, 2.8, 2.25, 2.25 and 3.05 respectively. It can be conclude that Yoma Bank has strong internal audit team and have implemented operational risk identification and assessment tools, taking the account of internal audit findings as an input to the various operational risk management tools. Likewise, Yoma Bank is using internal audit findings to compare management's risk and control assessments with the various operational risk management tools and continuously monitor the number of open and overdue internal audit finding and issues as a key indicator.

However R32 got mean score 2 only, that means Yoma Bank internal audit function not fully conduct a detailed end-to-end analysis of the operational risk profile assessment process, as well as assessments of process governance, the detail and quality of reporting, the process by which deficiencies are identified, tracked, and remediated, and whether the programme is functioning in a manner consistent with established policies in general.

R 36, R37, R38 and R39 relates to business process mapping and got mean score 2.5, 2.5, 2 and 2 respectively. It can be conclude that Yoma Bank Implement business process framework that provides guidelines for the creation of business process maps and undertake a risk-based approach to business mapping, implying a focus on high-risk processes rather than all business processes within the bank.

R40, R41, R42 and R43 relates to Key risk and performance measures and got mean score 2.05, 1.75, 2 and 2. It can be conclude that Yoma Bank is not establishing and uasing key risk and performance indicators at multiple levels throughout the bank, including at the group-wide level, the divisional level, and the individual business-line level.

Principle 7: Change Management

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to of change management. The respondents' perception on principle: 7 Change management's emerging and noteworthy practices of Yoma Bank is shown in Table (4.12).

Table (4.12) Principles 7: Change Management

Sr No	Practices No	Emerging and noteworthy practices	Mean
44	R44	Alignment of risk and control assessments, within the change management process, with the bank's operational risk taxonomy to allow for integration and aggregation of results within the bank's overall risk profile.	2

45	R45	A formal project governance programme that involves several approvals or "gates" through the life of a new product or initiative.	2.25
46	R46	The bank has defined objective criteria and procedures to identify new activities, products, technology systems, or business with geographically distant markets.	2.3
47	R47	The bank has clearly allocated roles and responsibilities for both the first and second lines of defence in order to assess the risk exposure relating to change initiatives in line with the accepted risk appetite of the bank.	2
48	R48	The identification of controls or actions required, either pre- or post-implementation, which are closely monitored by the second line of defence to ensure remediation.	1.75
49	R49	Establishing oversight committees to monitor the implementation of new product and new initiative frameworks as well as to review and approve specific business cases.	2.5
50	R50	Implementing a risk-based approach to the application of requirements for risk and control assessments, as well as approvals, such that products and initiatives subject to higher levels of risk and impact are subject to greater intensity of governance and oversight.	2.55
51	R51	A product risk framework that sets forth requirements at the various stages of the product life cycle (eg development, change, grandfathering and closure).	1.75
52	R52	Maintaining a central list of all the bank's products.	2.85
53	R53	Operational risk and control assessments related to new products and initiatives are performed by the first line of defence, and are subject to independent challenge by the second lines of defence.	2
54	R54	Appropriately formalised and documented involvement of several control groups within the second line of defence's review of risk and control assessments, such as finance, compliance, legal, business continuity, technology, and other risk management groups.	2.55
55	R55	Establishing a formal post-implementation review to assess the realisation of anticipated benefits such as cost reduction, revenue generation, and risk reduction prior to the formal closure of the project.	2.55

56	R56	A formal post-implementation review process exists to ensure effective implementation of new or material changes to products, activities, processes and systems.	2.55
57	R57	The bank reviews and updates the policy and procedures regularly, and/or on an event-driven basis, to take into account growth rates, technological developments, legal framework changes etc	2.55
Average			2.3

Source: Survey data (2019)

As described in the table 4.12, R44 R47, R53, got mean score 2. It can be conclude that Yoma Bank is not fully setting up alignment of risk and control assessments, within the change management process, with the bank's operational risk taxonomy to allow for integration and aggregation of results within the bank's overall risk profile. Likewise, new products and initiatives' operational risk and control assessments are not performed by the first line of defense and independence challenge by the second line of defense.

Regarding R45, R46, R49, R50 and R52 got mean score 2.25, 2.3, 2.5, 2.55, 2.85, respectively. It can be conclude that Yoma Bank has proper Product committee that approve new products and initiative through the life of products and initiatives. Beside, Yoma Bank also establish steering committee or oversight committee to monitor the implementation of new product and new initiative.

Regarding R54, R55, R56 and R57 got mean score 2.55 each. It can be conclude that Yoma Bank has appropriately formalised and documented involvement of several control groups within the second line of defence's review of risk and control assessments and also conduct post-implementation review to assess the realisation of anticipated benefits. Likewise, Yoma Bank also reviews and updates the policy and procedures regularly.

Principle 8: Monitoring and Reporting

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to of operational risk monitoring and reporting. The respondents' perception on principle: 8 monitoring and reporting's emerging and noteworthy practices of Yoma Bank is shown in Table (4.13).

Table (4.13) Principles 8: Monitoring and Reporting

Sr No	Practices No	Emerging and noteworthy practices	Mean
58	R58	Production of operational risk reports on a regular (ie quarterly or monthly) basis that are distributed to senior management and/or the board.	1.7
59	R59	Operational risk reports include an operational risk profile for the bank, including the inherent and residual risk levels for its taxonomy.	1.45
60	R60	Operational risk reports include details of key and emerging operational risks.	1.5
61	R61	Operational risk reports include an effective balance of qualitative and quantitative information.	1.5
62	R62	Operational risk reporting includes an appropriate balance of information related to changes in both the business environment and operational risk data (loss data, KRIs), and includes an update of key operational risk action items.	1.7
63	R63	Reporting of adherence to the operational risk appetite and tolerance.	1.25
64	R64	Inclusion of the operational risk profile in operational risk reporting, as well as key themes and issues identified through the use of operational risk management tools.	1.5
65	R65	Operational risk reports include key action plans to address material control gaps.	1.5
Average			1.51

Source: Survey data (2019)

As described in the table 4.13, R58, R59, R60, R61, R62, R63, R64 and R65 got mean score 1.7, 1.45, 1.5, 1.5, 1.7, 1.25, 1.5 and 1.5. it can be conclude that Yoma Bank not yet implement a process to regularly monitor operational risk profile, risk reporting and tracking market losses. Yoma Bank should develop operational risk reporting mechanism that operational risk reporting report, include operational risk of the bank and the inherent and residual risk levels for its taxonomy, to senior management or the board of director.

Moreover details of key and emerging operational risks, an effective balance of qualitative and quantitative information and an appropriate balance of information related to changes in both the business environment and operational risk data (loss data, KRIs) should be included in operational risk report.

Principle 9: Control and Mitigation

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to of operational risk Control and mitigation. The respondents' perception on principle: 9 Control and mitigation's emerging and noteworthy practices of Yoma Bank is shown in Table (4.14).

Table (4.14) Principles 9: Control and Mitigation

Sr No	Practices No	Emerging and noteworthy practices	Mean
66	R66	The use of metrics for comparison of returns (by business unit, by product) with the budget (projected outcome), fluctuation of daily P&L (specifically in trading/financing business unit) and specific transactions with an irregular return ratio.	2
67	R67	Clear assignment of both first and second line of defence responsibilities as they relate to the assessment and control of outsourcing risk.	2.05
68	R68	The use of operational risk management tools (ie RCSAs, KRIs etc) to help manage outsourcing risks.	1.3
69	R69	The development of contingency plans and alternative/ backup arrangements for material outsourcing arrangements.	1.3
Average			1.66

Source: Survey data (2019)

As described in the table 4.14, R66, R67, R68 and R69 got mean score 2, 2.05, 1.3 and 1.3. It can be conclude that Yoma Bank not yet established operational risk control and mitigation mechanism properly.

Although Yoma Bank have establish proper SOPs, SLA and SOD for certain products and services which include operational risk control and mitigation actions, however, not yet develop and use of operational risk management tools, such as risk control self-assessments (RCSAs), key risk indicator etc. Moreover, Yoma Bank should establish clear SODs and assignment to both first line of defense and second line of defense.

Principle 10: Resiliency and Continuity

The respondents were asked to rate and describe to what extent Yoma Bank have implemented the emerging and noteworthy practices related to Resiliency and Continuity. The respondents' perception on principle: 10 Resiliency and Continuity's emerging and noteworthy practices of Yoma Bank is shown in Table (4.15).

Table (4.15) Principles 10: Resiliency and Continuity

Sr No	Practices No	Emerging and noteworthy practices	Mean
70	R70	Well established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, and the establishment of thresholds for activation of business continuity plans (eg maximum tolerable outage etc).	2.8
71	R71	The integration of disruptive scenario analysis into other risk management tools and processes (eg KRIs, Pillar II etc).	2
72	R72	The provision of customised business continuity training to staff, according to their specific roles, as well as regular review of the training to ensure its applicability.	1.75
Average			2.18

Source: Survey data (2019)

Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. (BCBS 195, 2011. P17).

As described in the table 4.15, R70 got mean score 2.8. It can be conclude that, Yoma Bank develop business continuity programme, that is adequate with Yoma Bank nature, size and complexity, that include a well-established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, the establishment of thresholds for activation of business continuity plans.

However, R71 and R72 got mean score 2 and 1.7 respectively. It can be conclude that Yoma Bank not yet establish and integrate disruptive scenario analysis into other risk management tools and processes. Beside, Yoma Bank is not providing customised business continuity training to staff, according to their specific roles, as well as regular review of the training to ensure its applicability.

Yoma Bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Business continuity training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans.

CHAPTER 5

CONCLUSION

This chapter includes two main sections: findings on assessment of the compliance to the emerging and noteworthy practices of the Principles for the Sound Management of Operational Risk in Yoma Bank, suggestions and recommendation to make necessary corrective action to have robust and sound operational risk management practices.

5.1 Findings

This study has been conducted with the objectives of finding out Yoma Bank's operational risk management practices and compliance to the emerging and noteworthy practices of the Principles for the Sound Management of Operational Risk. To meet these objectives, a survey was conducted during November, 2019. Twenty senior management level executives, such as C Level, Head of department and Deputy Head of department, were selected to answer Questionnaire. All twenty respondents responded to the questionnaire. The questionnaire used in the study includes 3 parts: guidance for questionnaire ratings, respondents' demographic information and assessment of the ORMF with Emerging and noteworthy practices. The types of questions in the questionnaire are open questioned, closed questions, and 4 point Likert scale questions, which are aimed to analyze Yoma Bank's operational risk management practices compliance to the emerging and noteworthy practices of the Principles for the Sound Management of Operational Risk.

Based on the results from the analysis of respondents' demographic profile, it is found that 41 to 50 years of age group is the largest, followed by 36 to 40 years of age group, 51 to 60 years of age group, and so on. In gender composition, male is larger than female.

Based on the demographic information of respondents, it was found that most of the respondents are mature age level and educated persons. Therefore, they are able to analyze Operational Risk Management practices of Yoma Bank Limited. In addition, most respondents have been working in banking and finance industry for 10 years and over. Therefore, this study found that most respondents are knowledgeable in banking practices and they have good understanding in operational risk management practices.

Yoma Bank's operational risk management practices were analyzed with emerging and noteworthy practices results from review on BCBS's the principles for the sound management of operational risks. There are 72 emerging and noteworthy practices that relates to BCBS's 11 principles. And, each emerging and noteworthy practice is measured by 4 point Likert scale: 1 – Principle has not been implemented, 2 – Principle is materially not complied with, 3 – Principle is largely complied with and 4 – Principle is fully complied with.

Regarding Principle 1: Operational risk culture's emerging and noteworthy practices, Yoma Bank not yet established practices relate to compensation programme and remuneration that balance risk and reward and proper risk management training to all employees across the bank.

In Principle 2: Operational risk management framework culture's emerging and noteworthy practices, Yoma Bank not yet established proper operational risk management framework that comply with the The Principles of BCBS.

In Principle 3: Yoma Bank has strong corporate governance and board of director oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels. Also, board of directors are not reviewing and approve operational risk strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation.

In Principle 4: Yoma Bank's board of directors are not approving and reviewing the risk appetite and tolerance statement that capture the various operational risk appetites within a Yoma Bank and ensure that they are consistent.

In Principle 5: Yoma Bank's senior management not yet established and support appropriate operational risk governance structure, line of responsibility, sufficient corporate operational risk function (CORF) stature and operational risk committee.

In principle 6: Yoma Bank has strong internal audit team and have implemented operational risk identification and assessment tools, taking the account of internal audit findings as an input to the various operational risk management tools. Likewise, Yoma Bank is using internal audit findings to compare management's risk and control assessments with the various operational risk management tools and continuously monitor the number of open and overdue internal audit finding and issues as a key indicator.

Moreover, Yoma Bank internal audit function not fully conduct a detailed end-to-end analysis of the operational risk profile assessment process.

In principle 7: Yoma Bank is not fully setting up alignment of risk and control assessments, within the change management process, with the bank's operational risk taxonomy to allow for integration and aggregation of results within the bank's overall risk profile. Likewise, new products and initiatives' operational risk and control assessments are not performed by the first line of defense and independence challenge by the second line of defense.

However, Yoma Bank has proper Product committee that approve new products and initiative through the life of products and initiatives. Beside, Yoma Bank also establish steering committee or oversight committee to monitor the implementation of new product and new initiative.

Moreover, Yoma Bank has appropriately formalised and documented involvement of several control groups within the second line of defence's review of risk and control assessments and also conduct post-implementation review to assess the realisation of anticipated benefits. Likewise, Yoma Bank also reviews and updates the policy and procedures regularly.

Regarding principle 8 & 9: Yoma Bank not yet implement a process to regularly monitor operational risk profile, risk reporting and tracking market losses and not yet establish operational risk control and mitigation mechanism properly.

Regarding principle 10: Yoma Bank develop business continuity programme, that is adequate with Yoma Bank nature, size and complexity, that include a well-established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, the establishment of thresholds for activation of business continuity plans.

Moreover, Yoma Bank not yet establish and integrate disruptive scenario analysis into other risk management tools and processes. Beside, Yoma Bank is not providing customised business continuity training to staff, according to their specific roles, as well as regular review of the training to ensure its applicability.

5.2 Suggestion and recommendation

According to survey result, Yoma Bank need to improve in various aspect of operational risk management practices across all business and operation units to have sound Operational risk management framework.

For further improvement of the operational risk management practices, the following better practices need to be considered,

Yoma Bank should establish proper operational risk management framework, that clearly articulate operational risk management policies and procedures, implementation of the bank's operational risk taxonomy across all business lines and operational risk tools and Establishing a quality assurance programme to ensure that independent challenge and review, as applied by the second line of defence, results in consistent risk and control assessments.

Yoma Bank should regularly review the code of conduct and get approved by the board of directors. Moreover, Code of conduct should be available on the Yoma Bank's website.

Yoma Bank should have establish robust processes to manage operational risk across business and operation units. As part of the internal validation process, Yoma Bank should evaluate the aptness of its risk management framework and the effectiveness of its implementation.

Yoma Bank's board and senior management should have managed for approving material aspects of the overall operational risk framework. They should understand how operational risk affects the bank and comprehend the management reports submitted to them.

Yoma Bank should provide proper Risk Management training regarding operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities.

Yoma Bank should establish operational risk committee, to oversee all risks, to which a management level operational risk committee reports, with members who have expertise in banking business activities and financial as well as independent risk management.

Yoma Bank should develop operational risk reporting mechanism that operational risk reporting report, include operational risk of the bank and the inherent and residual risk levels for its taxonomy, to senior management or the board of director.

Yoma Bank should establish clear SODs and assignment to both first line of defense and second line of defense.

Yoma Bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Business continuity training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans.

5.3 Need for further research

Yoma Bank is already establish Operation risk management department for building Enterprise Risk Management Framework, ERM policy, procedures and practices.

However, the whole policy procedure and practices might need to review after certain period of time (one or two year) based on the outcoming and lesson leant during this period. So that Yoma Bank should perform further analysis on operation risk management frame work effectiveness with financial performance of the bank.

References

1. John C. Hull, Risk Management and Financial institutions, 2007
2. Peter S. Rose & Sylvia C. Hudgins, Bank Management and Financial Service, 2003
3. Abdullah Abdullah Aloqab Aloqab, Farouk Alobaidi & Bassam Raweh Raweh. (2018). Operational Risk Management in Financial Institution: An Overview. *Business and Economic Research, 2018, Vol. 8, No. 2*
4. Andersen, L.B., Häger, D.,Maberg, S., Næss, M.B., & Tungland, M. (2012). The financial crisis in an operational risk management context A review of causes and influencing factors. *Reliability Engineering & System Safety, 105*, 3-12.
5. Bitar, M., Naceur, M.S.B., Ayadi, R., & Walker, T. (2017). Basel Compliance and Financial Stability: Evidence from Islamic Banks. *International Monetary Fund.*
6. Central Bank of Myanmar FY 2018 Transaction Period Report (April to September)
7. DiRenzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D.,... Reinard, D. (2007). Operational risk management in financial institutions: Process assessment in concordance with Basel II. Software Process: *Improvement and Practice, 12*(4), 321-330. https://doi.org/10.1002/spip.322.
8. Ibrahimovic, S., & Franke, U. (2017). A probabilistic approach to IT risk management in the Basel regulatory framework: A case study. *Journal of Financial Regulation and Compliance, 25*(2), 176-195.
9. Basel Committee on Banking Supervision, (2011), Principles for the Sound Management of Operational Risk, retrieved from https://www.bis.org/publ/bcbs195.htm
10. Basel Committee on Banking Supervision, (2011), External Audit of Banks retrieved from https://www.bis.org/publ/bcbs280.pdf
11. Basel Committee on Banking Supervision, (2014), Review of the Principles for the Sound Management of Operational Risk, retrieved from https://www.bis.org/publ/bcbs292.pdf
12. WWW.CBM.GOV.MM
13. Yoma Bank Limited, Retrieved from https://www.yomabank.com/board-management-profile.php

Appendix A

List of Private Banks

Sr.No	Name of Bank	Date of Licence Issued
1	Myanmar Citizens Bank Ltd	25/5/1992
2	First Private Bank Ltd	25/5/1992
3	Co-operative Bank Ltd	3/8/1992
4	Yadanabon Bank Ltd	27/8/1992
5	Myawaddy Bank Ltd	1/1/1993
6	Yangon City Bank Ltd	19/3/1993
7	Yoma Bank Ltd	26/7/1993
8	Myanmar Oriental Bank Ltd	26/7/1993
9	Asia Yangon Bank Ltd	17/3/1994
10	Tun Commercial Bank Ltd	8/6/1994
11	Kanbawza Bank Ltd	8/6/1994
12	Small & Medium Enterprises Development Bank Ltd	12/1/1996
13	Global Treasure Bank Ltd	9/2/1996
14	Rual Development Bank Ltd	26/6/1996
15	Innwa Bank Ltd	15/5/1997
16	Asia Green Development Bank Ltd	2/7/2010
17	Ayeyarwady Bank Ltd	2/7/2010
18	uab Bank Limited	2/7/2010
19	Myanma Apex Bank Ltd	2/7/2010
20	Naypyitaw Sibin Bank Limited	28/2/2013
21	Myanmar Microfinance Bank Limited	2/7/2013
22	Construction, Housing and Infrastructure Development Bank Limited	12/7/2013
23	Shwe Rural and Urban Development Bank Limited	28/7/2014
24	Ayeyarwaddy Farmers Development Bank Limited(A Bank)	17/11/2015
25	Glory Farmer Development Bank Limited (G Bank)	8/6/2018
26	Mineral Development Bank Limited	6/7/2018
27	Myanma Tourism Bank Limited	9/7/2018

Appendix B

List of Foreign Banks

Sr No.	Bank Name	Date of Licence Issued
1	MUFG Bank, Ltd.	2/4/2015
2	Oversea-Chinese Banking Corporation Ltd	2/4/2015
3	Sumitomo Mitsui Banking Corporation	2/4/2015
4	United Overseas Bank Limited	30/4/2015
5	Bangkok Bank Public Company Limited	26/5/2015
6	Industrial and Commercial Bank of China	26/5/2015
7	Malayan Banking Berhad (Maybank)	27/7/2015
8	Mizuho Bank Limited	27/7/2015
9	Australia and New Zealand Banking Group Limited	29/9/2015
10	The Joint Stock Commercial Bank for Investment and Development of Vietnam (BIDV)	30/6/2016
11	Shinhan Bank	15/9/2016
12	E.Sun Commercial Bank Limited	27/9/2016
13	State Bank of India	27/9/2016

Appendix B

List of Mobile Financial Services Company

Sr.No.	Name of Company	Date of Registration CertificateIssued
1	Digital Money Myanmar Limited	28/9/2016
2	Ooredoo Myanmar Fintech Limited	26/7/2017
3	Internet Wallet Myanmar Limited	31/8/2017
4	Mytel Wallet International Myanmar Company Limited	18/10/2018
5	MPT Money Company Limited	1/10/2019

Appendix D

Operational Risk Management Framework of Yoma Bank Limited

This survey questionnaire is to use only for the research paper "A Study on Operational Risk Management Framework of Yoma Bank Limited" To Submit as a partial fulfillment towards the degree of Master of Banking and Finance (MBF) in the Department of Commerce, Yangon University of Economics.

❑- the square box indicates that question will have more than one answers, please selected all appropriate answers.

❍- the circle indicates that question will have only one answer please select only one appropriate answer.

Guidance for questionnaire ratings

Rating	Description
4 – Principle is fully complied with	The bank is entirely compliant with the principle, there is evidence to substantiate the assessment, and there are no outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties
3 – Principle is largely complied with	The bank is non-compliant in only minor aspects of the principle, the non-compliance is not deemed to be material overall and there may be some minor outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
2 – Principle is materially not complied with	The bank is non-compliant in major aspects of the principle, and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
1 – Principle has not been implemented	The bank is entirely non-compliant with the principle and there may be some outstanding non-compliance issues identified (eg issues raised through self-assessment or by groups such as internal audit, supervisors or other third parties).
0 – Not applicable	The Principle is not yet applicable to the bank.

Firstly, Thanks you for answering questionnaire.

I. Respondent's demographic Information

1. What is the range of your age?
   - ❍ 25-30 ❍ 30-35 ❍ 35-40 ❍ 40-50 ❍ 50-60
   - ❍ 60 above

2. Your Gender?
   - ❍ Male ❍ Female

3. Year in Banking and Finance industry.
   - ❍ Under Five Year ❍ 5-10 Year ❍ 10-20 Year ❍above 20 Year

6. Education.
   - ❍ High School ❍ Bachelor ❍ Master Degree
   - ❍ Ph.D ❍ Other (Specified) …………………..

II. Assessment of the ORMF with Emerging and noteworthy practices.

Principles	Emerging and noteworthy practices		Rating
1. Operational risk culture	1	The code of conduct or ethics policy applies to all the bank's staff and appointees, including members of the board of directors.	0 1 2 3 4
	2	The code of conduct or ethics policy is regularly reviewed and attested to by employees, is regularly approved by the board of directors, and is publicly available on the bank's website.	0 1 2 3 4
	3	Establishment and implementation of a whistle-blower programme.	0 1 2 3 4
	4	Linking the compensation programme and remuneration to risk-adjusted indicators.	0 1 2 3 4
	5	Establishing operational risk awareness for all employees; more advanced training on the operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities.	0 1 2 3 4
	6	Customised and mandatory operational risk training for many roles including business unit operations, supervisory levels, senior management, and the board of directors.	0 1 2 3 4
2. Operational risk management framework	7	The ORMF was reviewed and updated to ensure alignment following the publication of the enhanced *BCBS Principles for the Sound Management of Operational Risk* in June 2011.	0 1 2 3 4
	8	Referencing the relevant operational risk management policies and procedures.	0 1 2 3 4

	9	Applying the ORMF to all the bank's material operating groups and entities, including subsidiaries, joint ventures and geographic regions.	0 1 2 3 4
	10	The ORMF requires consistent implementation of the bank's operational risk taxonomy across all business lines and operational risk tools.	0 1 2 3 4
	11	Describing the roles and responsibilities of each of the three lines of defence as they relate to the use of the operational risk identification and assessment tools.	0 1 2 3 4
	12	Establishing the mandates, membership, and representation of various operational risk governance committees.	0 1 2 3 4
	13	Establishing a quality assurance programme to ensure that independent challenge and review, as applied by the second line of defence, results in consistent risk and control assessments.	0 1 2 3 4
	14	Creation of an operational risk dictionary that includes definitions and examples of the various operational risks in the bank's taxonomy. In addition, the dictionary includes guidance related to the classification of each of the operational risks within the taxonomy, to ensure consistent identification and classification across the bank.	0 1 2 3 4
	15	Establishing a control library to inventory all the controls within the bank and each of its business lines.	0 1 2 3 4
	16	Defining operational risk events beyond direct financial losses, so that such events include indirect losses such as forgone revenue and lost business, and reputational damage.	0 1 2 3 4
3. Board of directors	17	Establishing a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identifies acceptable business practices and prohibited conflicts.	0 1 2 3 4
	18	The board regularly challenges senior management on the design and effectiveness of the bank's operational risk management framework.	0 1 2 3 4
	19	The board reviews and approves an operational risk strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation.	0 1 2 3 4
	20	The board supports the establishment of a formal culture communications strategy, whereby senior management communicates the importance of strong risk management practices through a variety of forums such as employee communications and formal training	0 1 2 3 4

		sessions.	
	21	The board ensures that internal audit includes the ORMF as a focus within business unit audits, to complement the overall audit of the ORMF.	0 1 2 3 4
	22	The board ensures that the scope of internal audit's work on the bank's ORMF is not limited to risk measurement (ie model) activities and includes a sufficient focus on risk management activities.	0 1 2 3 4
4. Operational risk appetite and tolerance	23	Defining operational risk appetite and tolerance at both a divisional and taxonomy level.	0 1 2 3 4
	24	Utilising both quantitative and qualitative components within the bank's operational risk appetite and tolerance statement.	0 1 2 3 4
	25	Setting limits based on established key risk indicators such as loss metrics, deficiencies, events and residual risk assessments using operational risk identification and assessment tools that have been implemented.	0 1 2 3 4
5. Senior Management	26	Ensuring that an appropriate level of operational risk training is available at all levels throughout the organisation and that the training reflects the seniority, role and responsibility of the individuals for whom it is intended.	0 1 2 3 4
	27	Membership of the operational risk committee consists of the first line of defence, the CORF, and other second line of defence control functions.	0 1 2 3 4
	28	ORC meetings are convened regularly, minutes are prepared, and action items are tracked to completion.	0 1 2 3 4
	29	Succession plans for key operational risk individuals have been established to ensure continuation of critical operations and maintenance of expertise.	0 1 2 3 4
6. Risk identification and assessment	**Audit Finding**		
	30	The consideration of internal audit findings as an input to the various operational risk management tools (eg RCSAs, scenarios, key risk/performance indicators etc).	0 1 2 3 4
	31	The bank employs a process that considers audit findings in the challenging of business self-assessments.	0 1 2 3 4
	32	The bank's audit function conducts a detailed end-to-end analysis of the operational risk profile assessment process, including assessments of process governance, the detail and quality of reporting, the process by which deficiencies are identified, tracked, and remediated, and generally whether the programme is functioning in a manner consistent with established policies.	0 1 2 3 4

	33	The use of internal audit findings to compare management's risk and control assessments with the various operational risk management tools.	0 1 2 3 4
	34	The use of internal audit findings as an input to the regular updating of the bank's operational risk profile.	0 1 2 3 4
	35	Monitoring the number of open and overdue internal audit issues as a key indicator.	0 1 2 3 4
	Business process mapping		
	36	Implementing a business process framework that provides guidelines for the creation of business process maps.	0 1 2 3 4
	37	Undertaking a risk-based approach to business mapping, implying a focus on high-risk processes rather than all business processes within the bank.	0 1 2 3 4
	38	Establishing a central repository for all business process maps.	0 1 2 3 4
	39	Embedding the bank's operational risk taxonomy into the business process mapping methodology for aggregation and comparison with the operational risk profile.	0 1 2 3 4
	Key risk and performance measures		
	40	Establishing key risk and performance indicators at multiple levels throughout the bank, including at the group-wide level, the divisional level, and the individual business-line level.	0 1 2 3 4
	41	KRIs, KPIs and escalation triggers are subject to regular review and enhancement.	0 1 2 3 4
	42	The first line of defence creates action plans for metrics that breach their respective thresholds.	0 1 2 3 4
	43	The second line of defence independently challenges the selection of indicators and thresholds, as well as the proposed action plans.	0 1 2 3 4
7. Change management	44	Alignment of risk and control assessments, within the change management process, with the bank's operational risk taxonomy to allow for integration and aggregation of results within the bank's overall risk profile.	0 1 2 3 4
	45	A formal project governance programme that involves several approvals or "gates" through the life of a new product or initiative.	0 1 2 3 4
	46	The bank has defined objective criteria and procedures to identify new activities, products, technology systems, or business with geographically distant markets.	0 1 2 3 4
	47	The bank has clearly allocated roles and responsibilities for both the first and second lines of defence in order to	0 1 2 3 4

		assess the risk exposure relating to change initiatives in line with the accepted risk appetite of the bank.	
	48	The identification of controls or actions required, either pre- or post-implementation, which are closely monitored by the second line of defence to ensure remediation.	0 1 2 3 4
	49	Establishing oversight committees to monitor the implementation of new product and new initiative frameworks as well as to review and approve specific business cases.	0 1 2 3 4
	50	Implementing a risk-based approach to the application of requirements for risk and control assessments, as well as approvals, such that products and initiatives subject to higher levels of risk and impact are subject to greater intensity of governance and oversight.	0 1 2 3 4
	51	A product risk framework that sets forth requirements at the various stages of the product life cycle (eg development, change, grandfathering and closure).	0 1 2 3 4
	52	Maintaining a central list of all the bank's products.	0 1 2 3 4
	53	Operational risk and control assessments related to new products and initiatives are performed by the first line of defence, and are subject to independent challenge by the second lines of defence.	0 1 2 3 4
	54	Appropriately formalised and documented involvement of several control groups within the second line of defence's review of risk and control assessments, such as finance, compliance, legal, business continuity, technology, and other risk management groups.	0 1 2 3 4
	55	Establishing a formal post-implementation review to assess the realisation of anticipated benefits such as cost reduction, revenue generation, and risk reduction prior to the formal closure of the project.	0 1 2 3 4
	56	A formal post-implementation review process exists to ensure effective implementation of new or material changes to products, activities, processes and systems.	0 1 2 3 4
	57	The bank reviews and updates the policy and procedures regularly, and/or on an event-driven basis, to take into account growth rates, technological developments, legal framework changes etc	0 1 2 3 4
8. Monitoring and reporting	58	Production of operational risk reports on a regular (ie quarterly or monthly) basis that are distributed to senior management and/or the board.	0 1 2 3 4
	59	Operational risk reports include an operational risk profile for the bank, including the inherent and residual risk levels for its taxonomy.	0 1 2 3 4

	60	Operational risk reports include details of key and emerging operational risks.	0 1 2 3 4
	61	Operational risk reports include an effective balance of qualitative and quantitative information.	0 1 2 3 4
	62	Operational risk reporting includes an appropriate balance of information related to changes in both the business environment and operational risk data (loss data, KRIs), and includes an update of key operational risk action items.	0 1 2 3 4
	63	Reporting of adherence to the operational risk appetite and tolerance.	0 1 2 3 4
	64	Inclusion of the operational risk profile in operational risk reporting, as well as key themes and issues identified through the use of operational risk management tools.	0 1 2 3 4
	65	Operational risk reports include key action plans to address material control gaps.	0 1 2 3 4
9. Control and mitigation	66	The use of metrics for comparison of returns (by business unit, by product) with the budget (projected outcome), fluctuation of daily P&L (specifically in trading/financing business unit) and specific transactions with an irregular return ratio.	0 1 2 3 4
	67	Clear assignment of both first and second line of defence responsibilities as they relate to the assessment and control of outsourcing risk.	0 1 2 3 4
	68	The use of operational risk management tools (ie RCSAs, KRIs etc) to help manage outsourcing risks.	0 1 2 3 4
	69	The development of contingency plans and alternative/backup arrangements for material outsourcing arrangements.	0 1 2 3 4
10. Resiliency and continuity	70	Well established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, and the establishment of thresholds for activation of business continuity plans (eg maximum tolerable outage etc).	0 1 2 3 4
	71	The integration of disruptive scenario analysis into other risk management tools and processes (eg KRIs, Pillar II etc).	0 1 2 3 4
	72	The provision of customised business continuity training to staff, according to their specific roles, as well as regular review of the training to ensure its applicability.	0 1 2 3 4