A GUIDE TO RISK MANAGEMENT PROGRAMS

FOR BANKING INSTITUTIONS IN MALAWI

RESERVE BANK OF MALAWI

Preamble

The Reserve Bank of Malawi (RBM) issued Risk Management Guidelines in 2007 for the purpose of providing guidance to all banking institutions on risk management systems. These Guidelines were issued in the wake of its efforts to adopt and implement Risk Based Approach to Supervision. The RBM therefore issued a circular calling for risk management programs (RMPs) from banking institutions for assessment of their adequacy and effectiveness in the management of risks. The RMPs were accompanied by individual bank 'walk-through' presentations to ensure clarification of the submissions.

The review of the RMPs gave rise to the general observation that though most RMPs were adequate in some aspects, they demonstrated general weaknesses in some respects. It is in this regard that the RBM deemed it necessary to issue a guide that aims to provide guidance to banking institutions on key elements of a typical RMP. This guide is further meant to provide guidance, on an on-going basis, to new and existing institutions in preparing and developing their RMPs. The RBM will therefore endeavor to update this guide from time to time in order to ensure current and timely guidance.

Purpose of the Guidelines

The guide to Risk Management Program aims to provide banks with generic skeletal context of what should be contained. Nonetheless, banks are free to reflect their RMP in any format, and provide details that better communicate their risk management philosophy, practice and functionality. All efforts should be taken to ensure that the RMP reflects how risk is typically managed in the bank on a day to day basis.

Other Consideration

The RMP should not contain policies, procedures or manuals governing areas of risk. The RMP should however make reference to such policies and procedures to confirm existence of adequate and effective risk management procedures. In all, the RMP is expected to be a complete and stand alone document in itself to explain how risks are managed at the reporting bank.

Once again, the RBM appreciates efforts made by banking institutions in this initiative.

KEY ELEMENTS OF A RISK MANAGEMENT PROGRAM

Discussion of Main Activities and Plans of the Bank

The RMP should start with a description of the main activities and current plans of the bank in terms of customers, products, services, targets, number of branches, relationships with parent banks, if any, etc among others. This will provide a context for the risk discussion that follows. The approach should be that of an executive summary. However enough detail should be provided for the reader to understand the position fully, but excessive information should not be given. Further detailed information should be made available in other documents like polices and manuals that may be accessed at the bank, whenever necessary.

Discussion of Risk Appetite of the Bank

This divides naturally into two parts as follows:

Firstly, there is what may be called '***Business Risk Appetite***.' This covers the risks which the bank consciously takes as part of the business of being a bank. Credit, foreign exchange rate, liquidity and interest rate risks are obvious examples. The broad appetite should be spelt out here. For instance, how ready is the bank to grow its loan book, contemplate losses in the loan book, maximum exposure to a particular sector or industry among others. Linked risks should also be covered in high level terms, e.g. the interest rate and liquidity risks that arise from willingness to contemplate term lending funded from relatively short term deposits. Risks in treasury activities should be mentioned, whether the bank is a liabilities based operation or an asset based one, and what importance it places on diversified sources of income.

Secondly, there is what may be called the '***Non-Business Risk Appetite.***' This covers the risks that are not taken as a conscious way of earning money, but are incidental to the business. Risks such as operational, reputation and compliance (regulatory and legal) fall into this category. Unlike the business risks, which are, to varying degrees consciously sought out, these risks are ideally avoided. If they cannot be (which is usually the case), they must be transferred, or mitigated/controlled where possible. The broad approach should be outlined at the outset, with the details given under the specific risk headings later on. The ethical standards or culture that the bank follows could usefully be mentioned here since they impact on a number of risks (most obviously reputation and compliance).

Discussion of Strategic Risk

The purpose of this subsection is to provide an overall context of the activities of the bank and its risk appetites as outlined above to provide better

understanding of the bank and its risk perspective. A SWOT (strength, weaknesses opportunities and threats) analysis is a logical part of this, and this may be broken down into different business segments if need be. The bank should also cover how it deals with, or plans to deal with, current strategic risk, and how it will handle emerging causes such as a new competitor, whether foreseen or not. This discussion should naturally be part of the institution's business plan. As such, the Board should take a leading role, although, of course, senior management and the finance department will provide important input. As far as possible the discussion should also indicate strategy formulation, implementation and review processes including time frames for life and review of the strategic plan.

Discussion of Risk Management Framework

A thorough discussion of how risks are managed in the bank and the institution's risk management philosophy and practice should be covered here. This should cover the following:

- Organisational structure of the bank and the control arrangements that are embedded in it, such as segregation of duties and 'four eyes'[1] principle
- Role of the board and board committees
- Role of Management and management committees
- Mandate of the board and management committees
- Discussion of policies, procedures and limits; risk monitoring; and internal controls for each risk
- Role of the Risk Management function
- Role of the compliance function
- Role of Internal Audit
- Pin pointed risk owner of each risk and reporting lines
- Risk monitoring reports, their frequency and distribution

o ***Roles of the Board and Management***

The bank should be clear on the role of its board and management as per Risk Management Guidelines (RMGs) in managing risk.

[1] A requirement or arrangement where execution of a transaction significantly committing the banking institution, has to be done only after two authorized officers (at least) are agreeable to the transaction.

Senior Management set the detailed implementation policies for carrying out the strategy set by the Board. Further guidance may be obtained from the RMGs.

There should be an acceptable senior committee structure. Details can vary, but, broadly speaking, there should be, at a minimum, a Credit Committee, an ALCO, and a Risk Committee. Every committee should have clearly defined membership (i.e. those in attendance who participate in decisions), responsibilities and reporting lines.

o *The Role of Risk Manager*

It is worth spending some time outlining the role of the Risk Manager (RM) in order to ensure that both the RBM and banking institutions are clear as to what is involved. What follows to some extent covers the same ground as what is already contained in the Risk Management Guidelines, but, given the confusion that some banks appear to be having with this concept, some repetition may be useful.

The concept of banks having a dedicated Risk Manager is a relatively new one. Hitherto, risks have been managed in specific business units, such as credit or treasury, with any overarching review coming at the point of a high level committee, such as an Asset and Liability Committee (ALCO) where membership comprises some members of senior management.

In the interim such overlaps may still be accepted in smaller banks, given resource constraints, but there is much merit in banks having a dedicated Risk Manager, in addition to line managers for risk management.

The precise responsibilities of such a manager will, of course, depend on the bank, its activities and its organisational structure. The RM should be a member of the management team, (but not part of internal audit). Nevertheless, he should not detract line managers from the primary responsibility of managing risk in their respective business units. In broad terms, the RM's responsibilities should include to:

- Ensure that all risks assumed by the bank (old or emerging) are identified, measured (where possible), transferred (e.g. by insurance), avoided, and/or controlled/mitigated (e.g. by a limit structure). These risks include business risks, such as credit, which are an inherent part of banking, and non-business risks (e.g. operational risk) which is incidental to business in the banking institutions;
- Ensure that responsibility for day-to-day risk management is handled by a relevant manager (e.g. the Credit Manager), whose remit is clear and comprehensive;

- The RM will assign responsibility (liaising as appropriate with the Chief Executive) for any risks that are not being covered by the existing organisational structure;
- Identify any risks which transcend organisational boundaries and ensure effective liaison and coordination is in place. Business resumption plans are an example of this;
- Identify and put in place measures for dealing with risks in one area which will have an impact on other parts of the bank. For example, term lending by Credit and Marketing in a bank funded by short-term deposits will have interest rate and liquidity management impacts on the Treasury function;
- Ensure that all new business initiatives are subject to comprehensive risk assessment before roll out;
- Provide technical support to key risk committees, such as ALCO and Risk. The Risk Manager will be a member of the former and will normally chair the latter. He/she will also attend meetings of the Credit Committee and any other committee that there may be;
- Collate the aggregate risk position of the bank from various line functions and focus on high risk areas for corrective action by responsible risk owners;
- He/she will report to the Chief Executive and also be a member of the Management Risk Committee of the bank, if there is one. Such a committee may, in some cases, include the responsibilities of some of the specific committees mentioned above, particularly in smaller banks; and
- There must be no combination with internal audit, which has to remain separate with its own reporting line to the Audit Committee of the board.

o ***Internal Audit***

It is a check, external to management (including senior management), that risk management and compliance are working effectively, that all risks are being managed effectively and in accordance with the risk appetite, and that no unidentified or emerging risks have been missed. It provides assurance.

o ***Compliance Function***

The Compliance function is responsible for ensuring that all rules, laws and regulations (internal or external, financial or non-financial) are understood by all and implemented effectively.

Discussion of Risks Identified in RMGs[2]

The order in which the risks are dealt with is not important, although, given its importance and relative neglect in the past, it would be good to see Operational Risk given the prominence it deserves. The approach of the bank to each of the main elements (identification, measurement, monitor and control) of each risk should be outlined, together with how it is dealt with. A matrix showing whether the risk is deemed 'high risk, high impact,' or 'low risk, low impact,' or somewhere in between is often useful.

The aim here should be to give a high level outline of what the bank does, without, however, going into exhaustive detail. For example, there should be no need in this document to outline details of the classification and provisioning policies for non-performing loans. It should be sufficient to explain that there are such policies, that they are either in line with, or more strict than RBM guidelines, and explain at what level decisions are made, and who undertakes any necessary reviews. Reference can be made to the document in which full details are available, if required. However, roles of all players in the risk management of a particular risk should be fully covered, i.e. the board, board committees, management, management committees, risk owner, internal audit input should be spelt out.

More detail may be necessary under some risk headings that are less well known, and where management policies are less well developed (e.g. Operational Risk). Any other risks that the institution recognises, but which are not in the RBM list should, of course, also be covered. The bank should also provide details of all tools employed in monitoring risk such as maturity gap analysis and contingency plans.

It is important to treat each risk individually, even though such a risk could be contained by measures instituted for another risk. For example, it is advisable to treat reputation risk individually, just as any other risk identified in the RMGs.

Other Discussions

In conclusion, the document should also cover the following arrangements:

- ***Discussion of new product development***

Briefly explain the process involved to ensure the four key steps in risk management (i.e identification, measurement, monitoring and control) are fully taken care of before a new risk (i.e product/service) is taken on board.

[2] The RMGs identify the following risks: credit, strategic, liquidity, interest rate, foreign exchange rate, price, operational, compliance and reputation.

- ***Discussion of identified exceptional risk that has in fact been encountered***

How well did the institution's business resumption plans cope with an actual risk eventuality that was encountered eg fire, IT System breakdown. Briefly explain whether the institution has a risk review process which encompasses back testing; and how successful it has practically worked in the past. This discussion should also encompass business continuity plan and disaster recovery plan.

- ***Stress testing***

There is much merit in banks carrying out stress testing in various areas, as part of their risk monitoring. What exactly is needed depends on the bank and the risks it is dealing with. Examples of helpful stress tests are: changes in the level of non-performing assets, changes in interest rates, changes in depositor behaviour whereby they keep deposits with the bank for different periods of time, etc. It is recommended however, that stress tests and their methodology should remain within the ability of the board and senior management to understand.

Bibliography

1. Reserve Bank of Zimbabwe, Risk Management-Guideline No. 1-2006/BSD, 2006

2. Central Bank of Kenya, Risk Management Guidelines, August 2005

3. Bank of Tanzania, Risk Management Guidelines, August 2005

4. Bank of Uganda, Risk Management Guidelines, November 2002

5. Bank of Pakistan, Risk Management Guidelines for Commercial Banks & DFIs

6. Federal Reserve System, Guide for Risk Focused Supervision of Large Complex Institutions

7. Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, BIS publication, 2003

8. Community Bank Supervision Comptroller's Handbook, July 2003

9. Basle Committee, Basle Core Principles, October 2006

10. Basle Committee, Compliance and the Compliance Function in Banks April 2005