MANAGING OPERATIONAL RISKS IN A BANK: APPLIED RESEARCH IN MALAYSIA

Syed Syafudin Syed Abu Hassan
Accounting Research Institute and Faculty of Accountancy
Universiti Teknologi MARA, Malaysia

Rozainun Abdul Aziz
Accounting Research Institute and Faculty of Accountancy
Universiti Teknologi MARA, Malaysia

Abstract

This paper aims to offer better insights into risk management practices of a bank in order to mitigate its operational risks. Far from closely adopting the requirements and due to the nature of the risks faced by banks, this study investigates and observes how such framework is modified in practice to suit the nature and timing of operational risks.

Using the case study approach of investigation, we conducted our study in a bank in Malaysia and examined its risk management processes through interviews, documents and physical observations.

The paper highlights the implementation of a risk management program and summarises a record of related practices of how the bank manages its operational risks based on adaptation to Bank Negara Malaysia (BNM) guidelines and the Basel II committee paper. The findings will be useful to other banks to benchmark with their risk management program for enhancement purposes. It will also provide a guide as to how operational risks in a bank are managed effectively.

Keywords operational risks, banks, risk management, regulators, mitigation

Introduction

Risk or potential danger is unavoidable and it is present in virtually every situation. It is present in our daily lives, either at home or at work. Risk can also be described as a potential event that will prevent an organization from achieving its objectives (Australia/New Zealand Risk Management Standard, 2004). Basically, risk is related to the uncertainty of outcomes and the difficulty in identifying risks may differ from one situation to another (Pyle, 1997).

Risks in practice involve operational risks that might affect performance of an organisation if not managed properly. Risks are also difficult to measure and quantify in terms of their likely financial loss. Several regulations have been drawn up and established to address such difficulties and for the banking sector, the regulation called Basel II has classified banking operational risks into seven loss event types as per Table 1 below.

Table 1. Loss Event Type Classification (extracted from Operational Risk Guideline 2006)

Event-Type Category	Definition
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy which involves at least one internal party.
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law by a third party
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreement, from payment of personal injury claims, or from diversity and discrimination events.
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients including fiduciary and suitability requirements, or from the nature or design of a product.
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.
Business Disruption and System Failures	Losses arising from disruption of business or system failures
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

One of the crucial component of treating risk is to mitigate. There are six steps in a risk management process namely determining objectives, identifying risk, evaluating the risk, risk treatment, risk decision implementation and supervision and review are basic approaches in managing risks (Rejda, 2008). Determining the organization's objectives is the first step of the fundamental element in mitigating risks. Risks that are not identified are not likely to be mitigated. As such, they have to be identified so that evaluating of risks can be conducted accordingly to quantify the expected losses. The risk managers will have to make a decision on

which technique to be applied to mitigate risks. After implementing the technique(s), the risk management programmes need to be reviewed and assessed for improvement purposes.

On the other hand, Vaughan (1997) describes four techniques to treat the risk namely (a) avoidance, (b) reduction, (c) retention and (d) transfer. Different types of industry will have different types of risks and will entail different styles of managing it. For the banking industry, the effectiveness of managing risks plays an important role to the success or failure of the banks. Banks are now very complex and require regulators to place full-time examiners on-site, rather than conduct periodically regulatory examinations. This has created greater difficulty to keep a close watch on the activities of giant financial companies engaged in continually changing mix of activities. One factor that differentiates banks from many other firms is that banks are heavily regulated. Regulators especially Bank Negara Malaysia routinely examine banks and put pressure on those banks found to be excessively risky.

This paper is presented as follows. The next section will discuss briefly the research problem followed by the methodology adopted. Then, a brief introduction of the research site chosen and a description of the new Capital Accord (Basel II) are given since the case is adapted from this manual and the industry in which it operates is highly regulated. Next, we provide the findings and analysis of the mechanisms of risk management adapted by the case before presenting the conclusions.

Research Problem

The failure of a bank is normally caused by poor risk management system practised by a bank; cases like Barrings Bank and Socgen are now lessons to the banks to be more vigilant. Basically, in banks there are three important types of risk, i.e credit risk, market risk and operational risk. Market risk and credit risk are the most regulated risk and have comprehensively structured risk management. Methods of managing market risk and credit risk are fully developed and models have been put in place accordingly and reviewed regularly. However, operational risk methods to manage such risks are still under-developed. This is a relatively new field, so understandably, financial institutions have made less progress in developing formal models for practices. Therefore, recently regulatory bodies such as Bank Negara Malaysia (BNM) have emphasized standards regarding robust systems for operational risks.

Methodology

This study employed a case study method of investigation (Yin, 2004). The case identified and accessed is a bank in Malaysia whose operational risk management program was examined. This program is also based on the above six steps of the process, and observing research ethics, we withheld the name of the bank, and which we refer to as *the Bank* in our paper. Several documents issued by *the Bank* were referenced, but we could not list them in full as it would disclose the actual name of *the Bank.*

A simple triangulation method of collecting data was adopted in our study. Among the internal documents observed and accessed were Compliance Policy, Annual Report, Whistle Blowing Procedure, CAMEL Rating Methodology, Fraud Handling and Reporting Guideline, Risk Management Division, MASA Reporting Guideline from the Risk Management Division, Operational Risk Management Guideline and Policy, Risk Escalation Reporting Guideline. All these documents were supplied by *the Bank's* Risk Management Division. Interviews were conducted on an informal basis with employees from the same division, including senior officials. Again, due to confidentiality issues, the details of the employees involved are withheld too.

The New Capital Accord (Basel II)

In managing operational risks, *the Bank* has to comply with BNM requirements. BNM policies and guidelines on operational risks are adapted from the Basel Committee papers in relation to the capital measurement and standards framework for banking institutions. The committee comprise members from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States. The committee provides a forum for regular cooperation between its member countries on banking supervisory matters. Initially, the forum discussed modalities for international cooperation in order to close gaps in the supervisory net, but its wider objective has been to improve supervisory understanding and the quality of banking supervision worldwide by setting minimum supervisory standards especially in risk management and areas where they are considerable desirable.

A capital measurement system commonly referred to as the Basel Capital Accord (Basel I) was approved by the G10 Governors and first released to banks in July 1988 and continuously being revised, enhanced and evolved over time. This system provided for the implementation of the framework with a minimum capital ratio of capital to risk-weighted assets of 8% by the end of 1992. Since 1988, this framework has been progressively introduced not only in member countries but also in all other countries with active international banks including Malaysia.

Although the document has no legal status, most countries have adapted the Basel guidelines. In Malaysia, Bank Negara Malaysia (BNM), as the supervisory authority, has imposed on all Financial Institutions in Malaysia the requirement to comply with Basel I effective September 1989. During that time, the various financial institutions were subject to different capital adequacy requirements.

Under the New Accord (Basel II), there are slight differences from the previous accord (Basel I). It requires banks to maintain a minimum Risk Weighted Capital Ratio (RWCR) of eight percent at all times. The previous accord explicitly covers only two types of risks in the definition of risk weighted assets such as credit risk and market risk. Other risks are presumed to be covered implicitly through the treatments of these two major risks. But the New Accord, introduces treatment of operational risk that will result in a measure of operational risk being included in the denominator of a bank's capital ratio. The New Basel Accord, or Basel II created new guidelines for capital adequacy and risk management and Basel II was implemented in 2007.

The Bank's Organisation Structure

The Bank started operations in the 1980s with an initial authorized capital of RM500 million and a paid-up of RM80 million. Its authorised and paid-up capital was increased to RM2 billion and RM1.7 billion within 15 years to accommodate the growth of its assets and the expansion and growth of its operations. With a network of 90 branches nationwide, currently the bank is able to produce more than 50 innovative and sophisticated banking products and services, comparable to those offered by its conventional counterparts. Figure 1 shows the bank's risk management structure that highlights the overall process of risk management in *the Bank*. It should be noted that *the Bank* has a Risk Management Division to oversee risk management issues of *the Bank*. We now offer our findings in the following section.

Current Operational Risk Measurement

Our observations of the internal documents revealed the following. The operational risks were assessed based on their likelihood of occurrence and of impact to the business of *the Bank*. In general, operational risks exist without prior warning. The magnitude of impact and the likelihood of an event were assessed in the context of existing control. The likelihood of each risk occurring was examined according to whether the risk event is considered to be single or continuous in nature. Single events are those events that are not currently on-going but may happen as one-off events in the future. Continuous events are those that occur on a daily basis. In general, the impact and likelihood of operational risk are divided into 5 points as depicted in Table 1.

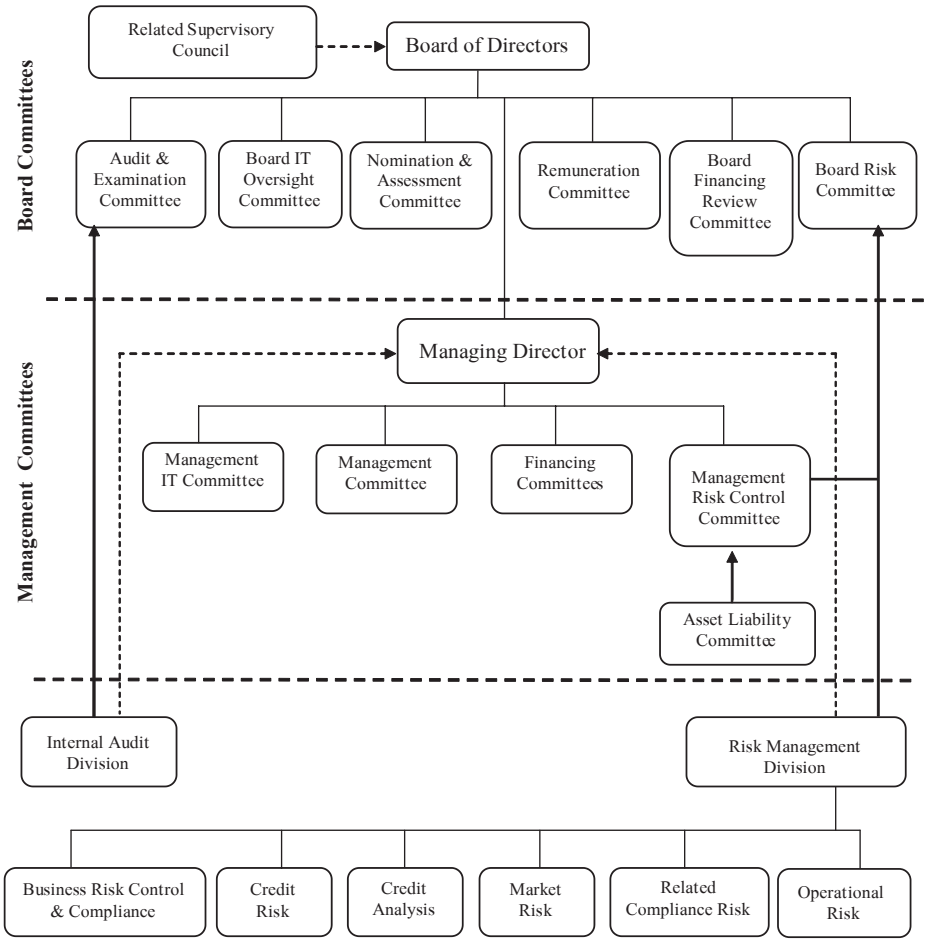

Figure 1: The Bank's Risk Management Structure (extracted from the Bank's 2007 Annual Report.)

Table 1: Risk Parameter (extracted from the Bank's own Operational Risk Guidelines 2006)

Risk Rating	Impact	Likelihood
5	Catastrophic	Very Likely
4	Major (Critical)	Likely
3	Moderate (Serious)	Possible
2	Minor (Marginal)	Rare
1	Insignificant (Negligible)	Unlikely

The risk parameter is a tool to measure the risk level of an event. The risk level is ascertained by taking into consideration both impact and likelihood of an identified risk. Thus, the equation to explain this relationship is as follows:

Risk Level = Impact + Likelihood.

By adding both risk parameters, the identified risk will be rated by using the five levels according to different colors to indicate urgency and attention that need to be addressed by *the Bank's* management. The application of these methods can be seen under fraud risk prevention program. The risk level is rated as given in Table 2.

Table 2: Risk Level (Extracted from the Bank's own Operational Risk Guidelines 2006)

Color	Total Score	Risk Level	Resolution Period
Red	8-10	High	Within 14 days
Orange	7-8	Medium-High	Within 30 days
Yellow	6-7	Medium	Within 45 days
Light Green	4-5	Medium-Low	Within 60 days
Green	2-4	Low	Within 90 days

The description of the risk levels is as follows:-

- High – Irreparable damage or catastrophic to the Bank.
- Medium-High – Serious long term damage likely and will become catastrophic if not mitigated.
- Medium – Inconvenience caused and will give short term negative consequences but without any serious long term damage.
- Medium-Low – Some inconvenience caused but without any short or long term negative consequences.
- Low – The impact and likelihood of the risk to happen is very minimal or the risk level is very negligible.

If the risk levels mentioned above are not resolved within the specified time, the person responsible or department must request for "extension" with proper justification and provide justification to Management Risk Control Committee (MRCC) meeting.

The Bank assesses its own vulnerability against operational risks via evaluating the effectiveness and adequacy of *the Bank's* internal controls, whether all prevention and detection aspects have been properly put in place. Good vulnerability evaluation will save *the Bank* in terms of investing into unnecessary internal control systems and resources. In order to assess the vulnerability of *the Bank* against the risks levels that have been assessed and measured, *the Bank's*

risk levels is measured against controls that have been put in place, as given in the following example:-

(Impact + Likelihood) – Controls in place = Vulnerability.

These controls values fall into three categories:-

- Highly Effective (HE) – The existing controls available are highly effective in addressing the operational risks as they reduce both/either the likelihood and/or the impact if the risks do occur.
- Moderately Effective (ME) – The existing controls available are moderately effective in addressing the operational risks because they only partially reduce the likelihood and/or the impact if the risks do occur.
- Ineffective (IE) – The existing controls available are ineffective in addressing the operational risks as they neither reduce the likelihood nor the impact if the risks do occur.

If the controls fall into the categories of ME and IE, the existing internal controls need to be reviewed, abolished, amended or replaced to make it highly effective.

Analysis of Findings

Within the banking system of this case, it is very important that the operations are run as smoothly as possible. However, as given earlier, operational risks exist without prior warning. Therefore, *the Bank* must manage those risks. The findings we present here address the issues concerned and discuss the risk management mechanisms that *the Bank* employs. Data were limited and where possible, the responses gathered were discussed and summarized accordingly. Then, we provide some insights into the risks concerned and associated mechanisms in place for current practices.

We identify four mechanisms of risk management undertaken by *the Bank* in order to manage those problems which are basically operational risks issues. These mechanisms are shown in Table 3.

It can be seen from the above that the 4 mechanisms for *the Bank* to manage their operational risks are as follows:

1. Operational Risk Capital Charges
2. Risk Based Audit Approach
3. Fraud Risk Prevention Program and
4. Management Awareness Self Assessment (MASA) Program

These mechanisms are assessed as to whether they can be used by *the Bank* to prevent them from suffering future losses. Operational risk capital charges are a requirement by Bank Negara Malaysia whereas, risk-based audit, fraud risk

Table 3: Summary of Operational Risks Issues, Risk Management Method and Impact

Current Problems	Risk Management Method	Impact
High operational risk capital charges of 20% means that a portion of the *Bank's* capital needs to be reserved for operational risk losses. *Bank* needs to maintain a minimum capital requirement for operational risk losses.	*Operational Risk Capital Charges*	Operational risk capital charges reduced to 8%.
Process risk Audit findings do not contribute to the added value to *the Bank* in terms of managing operational risks.	*Risk-based Audit Approach* – Compliance – based audit relies on the audit program and checklist. Risk level was determined by personal judgement of internal auditors.	Operational risks issues have not been examined in depth due to the absence of risk-based auditing.
People and Process risk Alarming figure of fraud cases and amount of losses.	*Fraud Risk Prevention Program* Fraud risk assessment has not been done. Bank has introduced whistle-blower reporting approach for mitigating fraud.	The whistle-blower reporting approach was implemented in March 2008 and yet to see an impact. However, it can be improved by outsourcing the service to the third party to enhance the effectiveness of the mechanism.
Process risk Resolving period for self-assessment issues did not achieve objectives within the time frame given, and was classification of risk level.	*Management Awareness Self-Assessment (MASA) Program*Bank has partially applied the risk management approaches. Identification and self assessment of risks were based on the modified risk level prescribed by the Bank.	Risk level determination is too rigid and has resulted in arguments and various resolving periods for each issue. In practice, due to the time constraints, the determination of risk level is based on the personal judgement of the staff.

prevention program system and MASA program were introduced by *the Bank's* management team to mitigate operational risks issues.

The next few sections will provide further discussions of these mechanisms, reflecting on their implementation in *the Bank*, based on interviews with personnels concerned and from viewing internal documents.

Operational Risk Capital Charges

In June 2007, BNM introduced a new Capital Adequacy Framework for banks and the approaches had been adapted from the Basel II Committee paper on "International Convergence of Capital Measurement and Capital Standards" published in June 2006. The capital adequacy framework for this particular type of bank, outlines three methods for calculating operational risk capital charges, namely:

i. The Basic Indicator Approach (BIA);
ii. The Standardised Approach (TSA); and
iii. Advanced Standardised Approach (ASA).

Currently, *the Bank* applies 'Basic Indicator Approach' in calculating operational risk capital charges and moves towards implementing 'Advanced Standardised Approach'. The impact of operational risks capital charges is to ensure that *the Bank* has the ability to absorb losses arising from the operational risks without affecting the financial performance of *the Bank* whilst enhancing its going-concern status. It is now becoming a requirement by Bank Negara for financial institutions to be more resilient in facing operational risks challenges and predicament by employing the mechanisms.

Identification and Quantification Issue

The issue of clarity with identification and quantification issues in relation to operational risks capital charges are apparent. Based on *the Bank's* 2007 annual report, the bank's risk weighted capital ratio stood at 12.69% amounting to RM9.78 billion comprising credit and market risk. This indicates that credit risk and market risk were well managed. There is no allocation for operational risk weighted ratio and also there is lack of disclosure on operational risks information in *the Bank's* annual report. This shows that *the Bank* is still unable to determine operational risk future loss and calculate its own operational risks exposure. Application of Advanced Standardised Approach models is an issue for *the Bank*. The paucity of operational loss data and the early stage of development of ASA models make it particularly difficult to address this challenging process. The availability of skilled staff may also be an issue, as it is important that bank's ASA models be adequately validated. This function must be done by suitably qualified parties independent of the development process to ensure they are conceptually sound and adequately capture all material risks.

The nature and quality of operational risk data collected affect not only the outcome of the bank's quantification process but also its operational risk management decisions. Basically, operational risk data under ASA approach

can be grouped into the following four categories namely (a) Internal data, (b) External data, (c) Scenario data, and (d) Data related to a bank's business environment and internal controls.

The Bank is currently in the process of identification and quantification of its operational risk data and since it is a daunting task as the scope is very wide, the outcome of the exercise has yet to be materialised. There are many issues in relation to identification and quantification of operational risk loss data faced by *the Bank*. As an example, some losses are clearly the result of operational risk but for others, it is less clear whether they should be classified as operational risk or credit, market or strategic risk. In other cases, it may be appropriate to allocate an individual loss partially to operational risk and partially to credit or some other risk category. These classification issues are broadly described as 'boundary' issues. Therefore, in determining the accurate classification of operational risk, *the Bank* needs to adopt the definition of operational risk as illustrated in the Basel II Committee Paper, which defines operational risk as the risk of loss resulting from inadequacy of failed internal process, people and system or from external events and this definition includes legal risk but excludes strategic and reputational risk. However, operational risk losses that are related to credit risk and have historically been included in *the Bank's* credit risk databases, e.g. collateral management failures will continue to be treated as credit risk for the purpose of calculating minimum regulatory capital under this framework.

Allocation of Internal Losses Issue

The other issue that raised concerns in calculating operational risk losses is related to the allocation of internal losses across business lines and event types. An individual operational risk event can lead to losses in multiple business lines and losses arising from a single event can sometimes span multiple event types. As in the case of events that trigger losses over a period of time, questions arise regarding how *the Bank* should treat these losses for risk measurement purposes and how they should be reflected in *the Bank's* internal loss databases. Allocation of losses that occur in a centralized business function or losses from a single operational risk event affecting multiple business lines could affect both its measurement and management of operational risk. For example, allocating a loss across multiple business lines and using this 'disaggregated' data for risk measurement would likely underestimate the risk where the losses were all a result of the same event.

From a risk management perspective, the failure to allocate such losses or inappropriate allocation could send the wrong signal to business line management and undermine the internal credibility of the capital allocation process. However, generally most banks have adopted one of two practices in this area, namely:

i. Allocating the entire loss to the business line for which the impact is greatest, or
ii. Allocating the loss on a pro-rata basis across the affected business lines. In the case of losses from a single event, the former practice seems to have been implemented more widely.

Risk Based Audit Approach

The second mechanism of managing operational risk is done by *the Bank's* Internal Audit Department (IAD) using the risk-based audit approach. Internal audit function plays an important role in detection and mitigation of operational risks in *the Bank.* In 2007, the internal audit decided to abolish CAMEL rating and introduced a general audit risk assessment applicable to branches, departments and subsidiaries, which is more simplified and generalised in terms that focus on operational risk. The audit risk areas have been pre set into four categories such as management oversight, adequacy of internal controls, compliance with regulatory requirements, policies and procedures and quality and integrity of financial data. Meanwhile, the risks levels are divided into low risk, medium risk and high risk and the final scoring is based on the four categories such as good, satisfactory, below standard and poor. The audit period for branches is within five working day, whereas head office departments and subsidiaries are within fourteen working days.

The above audit risks assessment is currently applied to *the Bank's* audit centers (branches, subsidiary and departments), except for credit department. Since the implementation of the new audit risk method, there has been much dissatisfaction showed by auditees on the rating given by auditors to them. There is lack of transparency in the disclosure of the audit risk rating and audit risk areas to the auditees especially branches. The determination of risk level was up to the professional judgement of the auditors and the risk scoring remains secretive. At the end of the audit exercise and after the close-up meeting, *The Bank* branches will get the end results of either good, satisfactory, below standard or poor, without knowing how the risks rating was determined. Under the previous CAMEL audit risk assessment, the risk level was determined and disclosed to the branches for their reference, and limited the gap for argument, however this method is no longer been practised. Actually, the reason for not disclosing the risk scoring to the auditees is to avoid argument on subjective matters particularly related to the determination of risk level. This has deprived the auditees the right to defend themselves and to argue on the scoring given to them.

As a conclusion to the risk-based approach, it is observed that *the Bank's* current practice of auditing does not adopt the operational risk assessment guidelines as

mentioned earlier. There is no structured risk assessment and quantification process prior to the audit work but on the contrary, the auditor depends fully on the audit program and checklist. As a result, the auditor has failed to disclose the root of the issues raised and this has affected the quality of the findings. By adopting compliance based auditing, the auditor will not be able to detect fraud effectively and *the Bank* will depend on the whistle blower reporting approach, or discover the fraud by chances.

Fraud Risk Prevention Program

This sub-topic explains the fraud risk prevention program that has been introduced by *the Bank* and also suggestions for the improvement of the method. Fraud risk is one of the main contributors to the bank's financial losses. Basel II committee paper explains that internal and external fraud are part of the seven operational risk loss event types that need to be identified, assessed and mitigated. *The Bank* is no exception to facing internal and external fraud problems. In March 2008, *the Bank* introduced the whistle-blowing procedure that was approved by Board Risk Committee later in the year, to enable any wrongdoing in a workplace to be tackled appropriately as part of fraud risk mitigation program. Thus, it can be an effective early warning system for *the Bank*. As such, it is of utmost importance that all *the Bank's* employees are vigilant about any work-related wrongdoings at their workplace and to promptly report such instances to the General Manager of Human Resource or Managing Director who can appoint officers from Risk Management Division as designated officers for immediate rectification and/or mitigation measures in minimising potential financial or reputation loss. *The Bank* gives the assurance that the reporter's identity will be protected.

The other effective mechanisms suggested to mitigate people risk are the development of ethics policy for staff and introduction of a pre-screening policy for new recruitment. Currently, *the Bank* follows the 'Code & Ethics' policy written by the corporate legal staff. These statements have several pages which define what constitutes improper and illegal behavior, including conflicts of interest, illegal gratuities, fraudulent statements, embezzlement, and a host of other nefarious activities. Despite having a good 'Code & Ethics' policy, *the Bank* needs to have a detailed pre-screening policy which is a good step in the fight against fraud.

It can be concluded that since fraud risk is difficult to predict and measure, the application of risk assessment methodology by *the Bank* on the fraud risk seems to be impracticable. *The Bank* can only rectify any loophole in work process after fraud was discovered. It is a daunting task for *the Bank* to study weaknesses in each work process for fraud risk assessment and prevention, where this may

require large human resources, it can be very costly and time consuming. Therefore, any fraud losses will be absorbed either by minimum capital requirement of operational risk or by transferring it to the insurance company. Normally, *the Bank* uses both approaches for managing fraud risk.

Management Awareness Self Assessment (MASA)

In 2005, *the Bank* introduced self-assessment with the objective of producing a comprehensive, credible and action oriented working culture. MASA is a program designed to develop a complete understanding and awareness of the operational risk that may arise from business or non-business operations activities within *the Bank*. MASA is used as a tool to report all operational risk issues including unresolved internal and external audit findings. In this regard, each reporting department or division is required to perform self-assessment on identified or discovered operational risk.

It was observed that the application of determining the risk level by calculating the impact and likelihood of the events was not practised by *the Bank* in the self-assessment process. This approach requires the branch manager to use his personal judgment guided by the risk descriptions above in order to determine the risk level. Branches did not apply the strict risk assessment approach since it consumes a lot of time and effort which will affect other work functions. Any non-compliance with guidelines will be strictly classified as high risk without measuring the frequency of the events and the impact from the non-compliance cases. Some of the non-compliance cases were isolated cases due to an oversight of certain procedures by staff. Sometimes, the risk that arises from non-compliance of certain steps in the guidelines is very low. It shows that practical aspects of risk assessment implementation in *the Bank* depart from theories and guidelines.

It can be seen that, in this self assessment practice, *the Bank* has partially applied the risk assessment method as stipulated in *the Bank's* operational risk guidelines. The classification of risk without adherence to structured risk assessment processes has resulted in inaccuracy in risk-level determination. *The Bank* also did not achieve the resolving period for most of the MASA high risk issues. It can be concluded that, based on the operational risk guidelines, the resolving period for high-risk issues should be shorter than the low-risk issue due to urgency reasons. On the contrary, in practice a high-risk issue requires more time to resolve rather than low-risk issue due to the complication of the issues. It is recommended that the resolving period for each issue needs to be reviewed. The time frame for each issue to be resolved must be achievable and based on the nature of each issue; therefore, it should not be based on the standard risk resolving period as per current practice.

Summary and Conclusions

Based on the four mechanisms namely Operational Risk Capital Charges, Risk-Based Audit Approach, Fraud Risk Prevention Program and Management Awareness Self Assessment (MASA) Program as described earlier, operational risk capital charges is a requirement by BNM for *the Bank* to improve operational risk management and detect potential financial losses as early as possible. The provision of operational risk capital charges has compelled *the Bank* to apply risk management methodology as per BNM guidelines and Basel II requirements. From the investors' point of view, they will be able to distinguish whether *the Bank* has been managed well or badly and they can use this knowledge to understand their portfolio strategy together with the calculation of the appropriate risk premium.

For risk-based auditing, *the Bank* did not apply the risk assessment method as embedded in *the Bank's* risk management policy but rather relied on *the Bank's* internal audit program which is more on compliance-based. This has made early detection of operational risk to be less effective and improvements need to be done on the internal audit approach by adapting risk-based auditing fully. This is where *the Bank* needs to revisit its process and respond immediately in order to improve their assessment exercises concerned so that such risks can be detected early.

The fraud risk prevention program also needs to be improved. Fraud cases were normally detected quite late, which indicates that *the Bank's* business work process needs to be tightened up and reviewed more regularly. However, with the introduction of the whistle-blower policy, it is hoped that it will minimise employee's intention to commit fraud. As for MASA program, the benefit received from the program to date in terms of highlighting operational issues by self assessment process has become an important mechanism for the Bank in identifying operational risks. Even though the application of risk management methodology is not comprehensive enough in *the Bank's* daily activities, but at least each employee of *the Bank* will be made responsible for part of the risk management program. Actually, the above four mechanisms are related to each other since those mechanisms apply similar risk assessment approaches. When *the Bank* fully enforces the risk assessment approaches in its internal auditing–fraud prevention program and MASA program, this will eventually help *the Bank* to identify and quantify its potential financial losses exposure, minimising operational risk capital charges.

Based on this study, it can be concluded that in order for risk management to be effective, continuous monitoring and appropriate inspection and rectification should be part of the package to manage operational risks. Human intervention also plays a significant role in any enforcement in risk management practice; all these, as seen in the observation of *the Bank's* practice described earlier. However,

operational risks are harder to quantify and model than market and credit risks. Currently, the improvements in all banks' management information systems and computing technology have opened doors to improved operational risk measurement and management. Over the next few years, other banks and regulators will continue to develop better approaches for operational risk management. For *the Bank*, 2008 meant compliance with Capital Adequacy Framework as prescribed and Business Continuity Management Guidelines issued by Bank Negara Malaysia. More compliance requirements would probably lead to a more controlled operating environment; therefore, the Bank's management should not compromise on operational risk management. On the contrary, risk management would play a pivotal role in the bank's pursuit to introduce various changes within the bank.

This case study research also implies has indentified three areas of significance in managing operational risks in *the Bank*. Firstly, even though their practices attempt to apply theory and methods outlined by Basel II and BNM guidelines, a compromise needs to be made with some adjustments to the operational risk management methods in order to conform to *the Bank's* practices. Secondly, since the scope of operational risks is broad and encompasses the whole *Bank's* organisation structure, it is important that every person in the organisation understand the overall concept of operational risk and the six general structured processes of risk management as discussed earlier must be inculcated in the day-to-day business activities.

In general, the risk management skills should not be limited to certain departments or just a few employees only. Everyone in the organisation should be well-trained and properly guided to practise the mechanism implemented. Employees should also comply with the risk management policy and guidelines in managing the operational risks. Finally, since the operational risks are difficult to identify and quantify, the cost and benefit of such training need to be evaluated prior to implementation for any mitigation aspects particularly in terms of risk decision, either transfer avoidance, retention or reduction of the risk. For example, by transferring the risk to the insurance company, the cost of premium paid must be less than the cost of retention. Failure to conduct a detailed cost and benefit study on risk decision will result in the bank incurring additional unnecessary cost.

For operational risk management to achieve its objectives, it is recommended that each employee in the organization needs to know, understand and take responsibility for managing risk. It should be everyone's concern and responsibility, not specific to a group of staff such as Risk Management Division or the top management of the bank only. It should form the bank's working culture whereby identifying and managing risks is part and parcel of all employee's daily decision making process.

They need to anticipate what might go wrong before any problem arises. The bank's management may not have insight into what could go wrong but with the help of every employee in the bank by taking up responsibilities for risks within respective areas of responsibilities, any potential catastrophe could be avoided. Hence, we suggest that future work should examine the role of employees in operational risk management that will create an impact on risk management in the banking industry.

Acknowledgement

The authors would like to thank Prof Dr Ibrahim Kamal Abdul Rahman, Dean of Faculty of Accountancy, and Prof Dr Normah Hj Omar, Director of Research Institute, for their continuous support and encouragement for us to "write and write" continuously for our career development.

Bibliography

Anthony, M. and Santomero (1997). Commercial Bank Risk Management- An Analysis of The Process.

Association of Certified Fraud Examiners (ACFE's) (2004). National Fraud Survey on the Effect of Occupational Fraud. US.

Australia/New Zealand (2004). Risk Management Standard, AS/NZS 4360: 2004.

Basel Committee of Banking Supervision (2004). *Implementation of Basel II: Practical Consideration*, Bank of International Settlements.

Bank Negara Malaysia (2004). *Audit Examination Report*.

Basel Committee on Banking Supervision (2005). *Compliance and the Compliance Functions in the Bank*, Bank of International Settlements.

Basel Committee on Banking Supervision (2001). *Conducting a Supervisory Self Assessment Practical Application*, Bank of International Settlements.

Basel Committee on Banking Supervision (2006). *Core Principle for Effective Banking Supervision,* Bank of International Settlements.

Basel Committee on Banking Supervision (2007). *History of Basel Committee and its Membership*, Bank of International Settlements.

Basel Committee on Banking Supervision (2006). *International Convergence of Capital Measurement and Capital Standards*, Bank of International Settlements.

Basel Committee on Banking Supervision (2006). *Observed Range of Practice in Key Elements of Advance Measurement Approach (AMA),* Bank of International Settlement.

Basel Committee on Banking Supervision (2003). *Operational Risk Transfer Across Financial Sector,* Bank of International Settlements.

Basel Committee on Banking Supervision (2007). *Principles for Home- Host Supervisory Cooperation and Allocation Mechanisms in the Context of Advance Measurement Approach (AMA)*, Bank of International Settlements.

Basel Committee on Banking Supervision (2003). *Sound Practices for the Management and Supervision of Operational Risk,* Bank of International Settlements.

Basel Committee on Banking Supervision (2003). *Sound Practices for the Management and Supervision of Operational Risk*, Bank of International Settlements.

Basel Committee on Banking Supervision (2001). *Working Paper on the Regulatory Treatment of Operational Risk*, Bank of International Settlements.

Enterprise Risk Management Committee (2003). *Overview of Enterprise Risk Management.* Casual Actuarial Society.

KPMG, (2004). *Fraud Survey Report*. Forensic Accounting and Investigations Advisory Services.

KPMG, (2007). *Risk Survey*. Business Advisory Services Research.

McAdams and Arthur C. (2004). *Security and Risk Management: A Fundamental Business Issue.*

Mohamad Azhar H. (2006). An overview of basel committee paper entitled enhancing corporate governance for banking organization. *The Bank Risk News.*

Pyle, D. H. (1997). *Bank Risk Management Theory.* Research Program in Finance Working Papers RPF-272.

Redja, G. E. (2008). *Principles of Risk Management and Insurance*.

The Bank (M) Berhad Risk News (2006). Retrieved January 18, 2008 from The Bank Risk Management Portal.

The Bank's (2005). *Shariah Compliance Policy*.

The Bank's (2007). *Annual Report*.

The Bank's (2007). *Whistel Blowing Procedure*.

The Bank's (2003). *CAMEL Rating Methodology*, 2003. Internal Audit Division.

The Bank's (2006). *Fraud Handling and Reporting Guideline*, Risk Management Division.

The Bank's (2006). *MASA Reporting Guideline*. Risk Management Division.

The Bank's (2006). *Operational Risk Management Guideline.* Risk Management Division.

The Bank's (2006). *Operational Risk Management Policy*. Risk Management Division.

The Bank's (2006). *Risk Escalation Reporting Guideline*, Risk Management Division,

Vaughan, E. J. (1997). *Risk Management*. University of Iowa, Willey USA.