CHAPTER FOUR

THE RISK BASED AUDITING METHODOLOGY ADOPTED

4.1 Risk Based Auditing Methodology Adopted By The Internal Audit Department Of ABC Bank

The change from traditional auditing approach to risk-based auditing approach was spearheaded by the Audit Committee of the Board (ACB) of ABC Bank. The reasons behind such change was that firstly, the ACB was looking into possible means in order to perform the routine internal audits in a more efficient, effective and economical manner. Secondly, the ACB recognized the fact that in order for the internal audit function to create or add value to the organization, the traditional way of auditing need to be further enhanced. Hence, the risk-based auditing approach was considered. Furthermore, the ACB realized that although there was some form of risk assessment and risk-based auditing methodology performed in the past, this approach may not be comprehensive and not in line with the best practices as promulgated by the Institute of Internal Auditors (USA). As a result, a team of consultants was employed by ACB to introduce and customize the risk-based auditing methodology for ABC Bank. The consultants were required to customize the risk-based auditing methodology and to train the methodology for a period of three months to a primary batch of key personnel auditors. These auditors are then tasked to subsequently train the rest of the internal audit department.

This section discusses the key activities adopted under the risk-based auditing methodology by ABC Bank. Figure 3 illustrates that the RBA methodology adopted is in line with the best practices stipulated by the Institute of Internal Auditors (IIA) standards. The IIA is an international professional body. Statements of internal auditing standards and practice

guidelines are considered best practices for the internal audit profession worldwide.

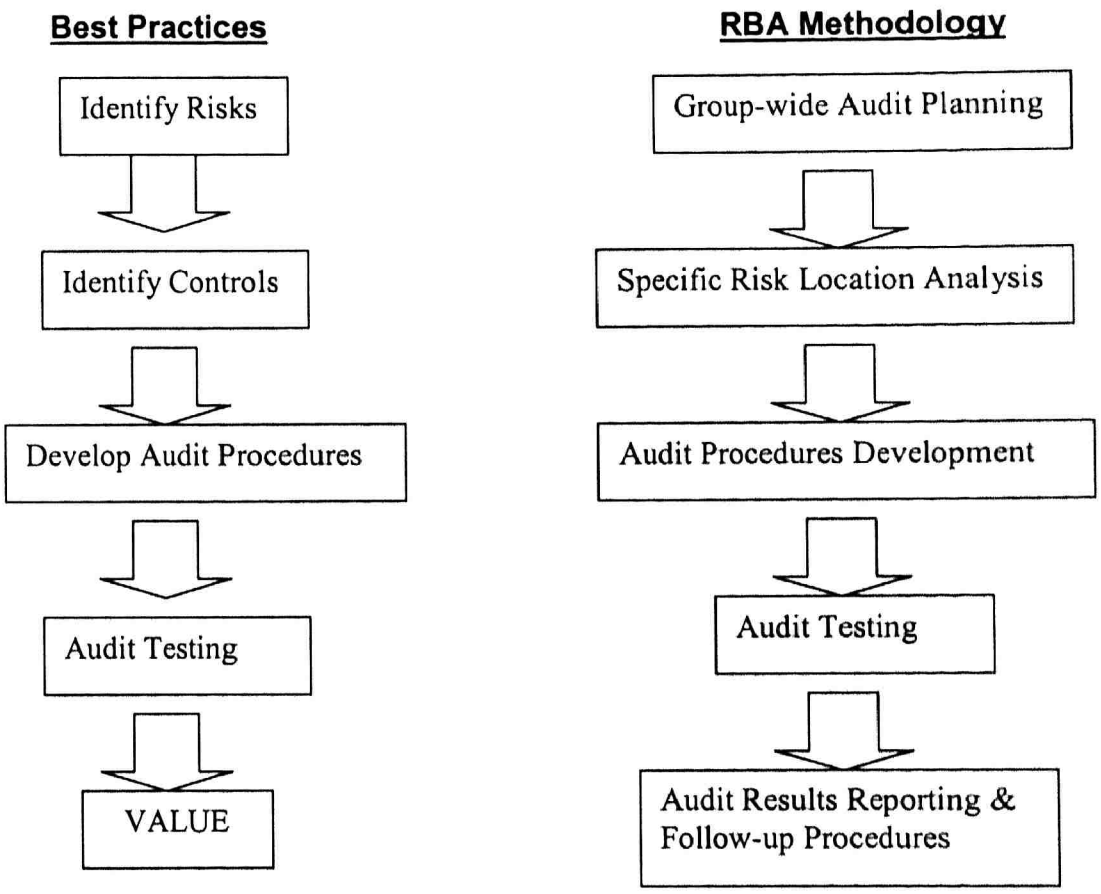


Figure 3 : Comparison Between The Risk Based Auditing Methodology and Best Practices

4.2 Group Wide Audit Planning

During the Group-Wide Audit Planning stage, the annual audit plan is prepared and tabled to the ACB of ABC Bank for their approval and endorsement. In the Group-wide audit planning stage, the involvement of the senior management level of the internal audit team is required to further analyse and breakdown the risk prevalent in ABC Bank. The involvement of the senior level management assists in the classification of the risk identified according to its severity and extremity. Risk can be

defined as anything that could jeopardize the achievement of the organization's objectives. Here, the management of the internal audit department discusses the risks with the line managers as well as with the CEO of the organization to further understand the risks faced by the financial institution. From the discussions with the senior management of the organization and based on past knowledge, the crucial risks areas can be readily identified. Typically, the risk profile of ABC Bank should include credit risk, liquidity risk, market risk, foreign exchange risk arising from ABC Bank's foreign operations and foreign exchange trading, customer satisfaction risk, data integrity risk, security risk as the bank provides internet banking services and operational risk.

In addition, under the Group-wide Audit Planning activity, the broad goals of the organization are scaled down to each of its measurable objectives. Subsequently, the risks that could affect the success of the organization in achieving its objectives are listed down according to its priority in relation to its significance. The objectives of the organization may be in terms of market share, customer satisfaction, employee relations, compliance with laws and regulations, financial position and results, or a myriad of other areas. Among the consequences for not addressing these objectives are lost market share, customer dissatisfaction, inappropriate product pricing, low employee morale, failure to comply with relevant laws and regulations or fraudulent financial reporting. Upon identifying the risk, the next thought process should include the root cause of why the risk might be realized as well as the effect of the risk, that is, the harmful consequence or opportunity lost when the risk is realized. The risk should be quantified, if possible. If it is not quantified, it should at least be expressed in specific and concrete terms.

To facilitate identification of risk, the use of risk inventory is vital. A risk inventory is a comprehensive list of the types of risks that could threaten

the organization as a whole, or specific processes within the organization. Risk inventory provides a common language for the internal auditors to communicate with each other and with the auditees as well as the Audit Committee of the Board in the risk identification and assessment process. It eliminates the need to explain at length when a particular risk is being examined, and reduces the likelihood of miscommunication.

Whether the risks would be incorporated in the organization's risk profile depends on whether they can be substantiated with facts, past records and relevant statistics. These risks would be subjected to further discussion and confirmation with auditees to obtain a better, non-biased and well-diversified view or perception. The risks identified are subsequently prioritized based on their significance of impact on the organization and their likelihood of occurrence over a period of time. In prioritizing the risks identified, a voting technology is used whereby the head of departments/sections/base managers are requested to vote anonymously based on two factors namely, the significance of the impact of the risks if it occurs and likelihood of the risks occurring, using the voting technology. In this way, group think can be eliminated and an independent assessment on the risk can be accomplished. In evaluating the risks, the head of departments and section heads as well as base managers are requested to only consider the inherent risks, that is, without considering the processes or controls in place to manage the risks. Table 5 shows the criteria to evaluate the prioritization of risk based on the two factors, that is, likelihood and significance.

Category	Likelihood	Significance
Low	Unlikely risk will occur	Probably will not materially impact the attainment of objective if the risk occurs
Medium	Somewhat likely the risk will occur	May impact the attainment of the objective if the risk occurs
High	Likely risk will occur	May significantly impact the attainment of the objective if the risk occurs

Table 5 : Evaluation Criteria In Risk Prioritization

Once the risks have been incorporated into the risk profile and had been prioritized accordingly, the target process or the key activities and functions that could have an impact on the risks are then determined. The risk locations where these functions, key activities or target processes are then determined and incorporated into the annual audit plan accordingly.

4.3 **Specific Risk Location Analysis**

Based on the group-wide audit plan, the field auditors are required to audit the risk locations identified and to test the strength of the design of controls relevant to the risks identified by the audit management of ABC bank during the Group-wide audit planning stage. Here, understanding of the functions to be audited is crucial in order to comment on the adequacy of the design of controls relating to the risks identified. Examples of factors used to assess the strength of the controls are:-

- whether there are or they are pervasive controls versus specific controls or monitoring controls
- are the controls preventive or detective in nature
- are the controls system based or people based
- do controls leave audit trails for tracking purpose
- how do the auditors rate the design of the controls when benchmarked against industry practices or best practices

The cost-effectiveness of the controls in place is also commented at this stage. What this means is that there is a need to balance risks and controls. Naturally, high risks areas should be mitigated or managed by controls that are strong. On the other hand, if a risk area is considered low, it should not be managed by excessive controls. This is because excessive controls could result in reduced productivity, increased bureaucracy, increased turnaround time and increased complexity.

At this stage, flowcharts, internal control questionnaires or other forms of templates in documenting risk and controls are used depending on effectiveness and requirement basis.

4.4 Audit Procedures Development

Audit procedures are developed based on the auditors' assessment on the present design of the controls pertaining to the risks in order to test the operating effectiveness of the controls. Audit procedures will determine the audit scope and coverage and extent of testing for each risk location. The audit procedures list down all audit tests that has to be performed by the auditors to assess the operating effectiveness of the controls in place for a particular business process. At this stage, the type of audit procedures for example, interviews, vouching and verifying, inspection and observation or facilitated meetings are used. The determination of the audit procedures to test the controls are dependent on which audit procedures would most likely produce results in the most effective and efficient manner.

4.5 Audit Testing And Reporting

At this stage, auditors are required to perform tests according to the audit procedures developed. For instance, one of the audit procedures developed for a purchasing department requires the internal auditors to vouch payment vouchers against original invoices. In his audit testing, the

internal auditor will select a sample of payment vouchers and vouched them against original invoices and any discrepancies will be noted. Based on the audit testing, the field auditors are required to analyse the results of testing, determine the implications of the audit findings, analyse root causes of the audit findings noted and develop recommendations to further improve the control environment. During the fieldwork, the auditors are also required to provide feedbacks on any potential risks not originally included in the organization's risk profile to their managers for further deliberation.

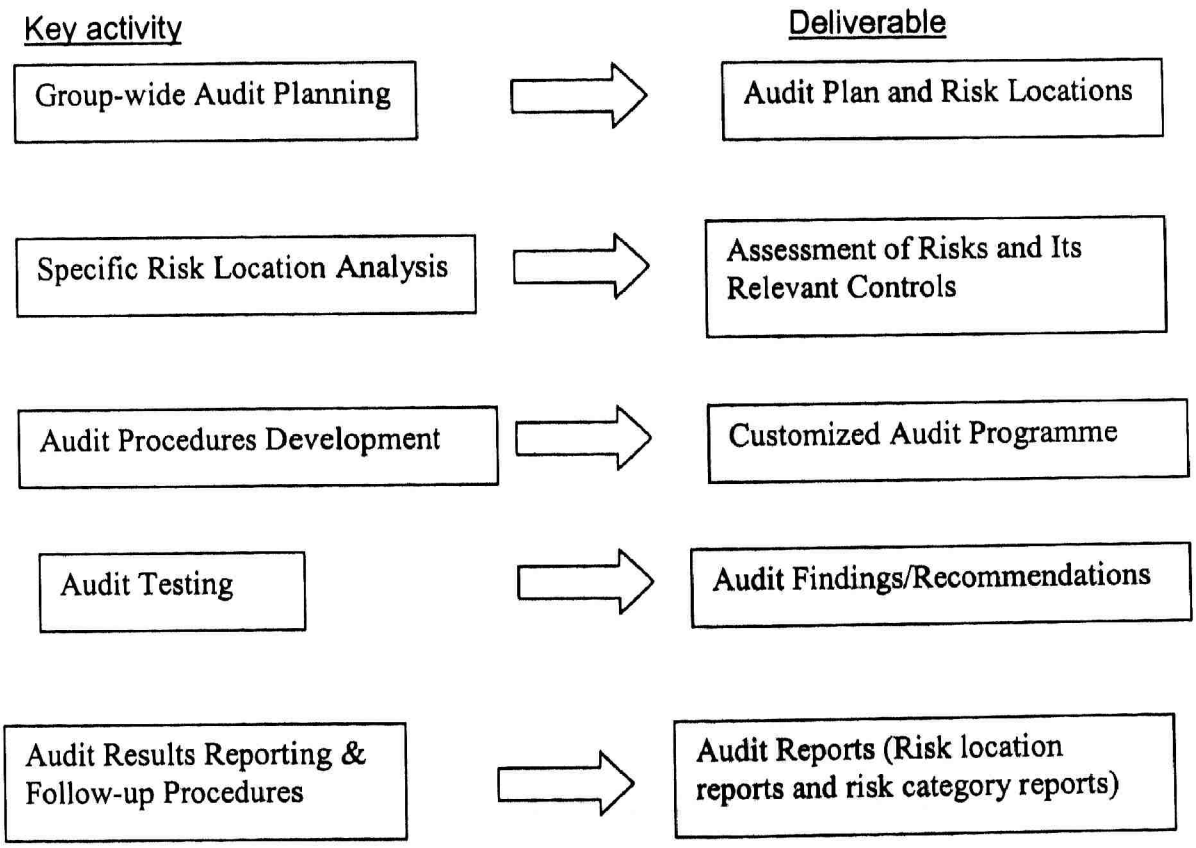
There are three types of reports presented to the Internal Audit Committee and Audit Committee of the Board. The first report is based on the risk location and the second report is based on the management of the risks after testing the relevant controls. Risk location reports would be prepared at the end of each audit visit. Risk reports (which summarises the findings of all the relevant locations in relation to an identified risk, for example, credit default risk) would be prepared in the appropriate intervals in accordance with the risk priorities, that is, half yearly for extreme risk areas, annually for high risk areas, 18-monthly for moderate risk areas, once in 36 months for low risk areas. The third type of report which is called the Group-wide Audit Report is prepared at the end of the financial year. The group-wide audit report would be prepared to provide a global view of all the risks identified for internal audit purposes and their assessed state of controls from the audit works performed in the past one year. This will also facilitate the organization in coming out with the "Statement Of Internal Controls" by the directors as required by the listing requirements of the KLSE.

Follow-up on the management actions' on the audit exceptions and recommendations will be reported to the Audit Committee of the Board on a periodic basis.

Continuous feedback and evaluation are needed in order to update the risk profile of ABC Bank as risks are continually evolving into different forms and do not remain stagnant. Furthermore, feedback will be obtained to determine whether the risk reports need to be prepared at a shorter interval, that is, while the audit visits of all the relevant locations are being completed.

Figure 4 presents the main result or deliverable for each key activities of the RBA approach of the internal audit department.

Figure 4 : Key Activities Of The RBA Approach and The Respective Main Deliverable



4.6 Existing Audit Approach of the Internal Audit Department Against The Risk Based Auditing Approach

Table 6 illustrates the differences between the existing audit approach against the RBA approach.

Table 6 : Comparisons Between the Risk based auditing approach and the existing auditing approach at ABC Bank

Audit Factors	Risk-Based Auditing Approach	Existing Audit Approach
Methodology	Application of top-down methodical approach for risk assessment and identification	Audit visits of all auditable units identified from audit universe with rotational basis fixed at intervals of 18 months
	Require exercise of judgement in a structured manner from the auditors	'Mechanical' approach based largely on the standard audit programmes
	Use of common language (Risk Inventory) in the risk identification and assessment process	Risks are not defined
Planning	Significant involvement and input from the Chief Internal Auditor and management level of the internal audit department as well as senior auditors in the group-wide audit planning stage. The	Audit planning is done for each location and the approach taken depends on the respective Heads of Department in Audit Division (fragmented approach).

Audit Factors	Risk-Based Auditing Approach	Existing Audit Approach
	planning involves comprehensive risk identification and assessment activities to highlight risks and locations.	
Audit Cycle	Frequency of audit visits is dependent on risk prioritised as extreme, high, moderate and low based on the significance of risks and likelihood of their occurrence over a three year audit plan.	Frequency of audit is based on yearly audit plan with fixed rotational intervals of 18 months.
Audit Approach	A risk-based approach where risks are systematically identified, assessed and prioritized. Subsequent audit work would be focused on the review of relevant processes and to identify risk controls as well as its operational effectiveness.	Essentially a compliance-based audit based on Standard Practice Instructions established by the organization. The current reporting requirements under previous auditing approach is not risk-driven.
Audit Procedures	Customized audit procedures are developed to test the effectiveness of operational controls	Existing audit procedures specially developed for branches based on the standard practice

Audit Factors	Risk-Based Auditing Approach	Existing Audit Approach
		instructions. They are homogenous for all locations.
Control Assessment	Controls are assessed on two aspects namely : (a) control designs and (b) their operating effectiveness	To ensure that the auditees comply with the standard practice instructions of ABC Bank and no assessment on the design of controls is performed.
Audit reporting	There are 4 (3 plus 1) different types of audit reports , that is, (1) risk location report (2) risk category report (3) group-wide audit report (4) supplementary – interim report	A standard audit report with rating "satisfactory" or "unsatisfactory" given to each auditable unit.
	A central quality assurance review (QAR) function for audit reports is to be instituted.	Respective Heads of Departments and Base Managers are reviewing audit reports and there is no specific parameter set to determine the quality of the reports.
Monitor/Follow -up	Formalized continuous improvement monitoring process is in place and the effectiveness of the audit	Follow-up on outstanding audit findings will be done every quarterly. Reasons for non-rectification

Audit Factors	Risk-Based Auditing Approach	Existing Audit Approach
	recommendations. This would include the identification of improvement indicators after the audit.	submitted by the auditee will be reported to the ACB accordingly.

4.7 **Feedback From Auditors of the Internal Audit Department**

A list of open-ended questionnaires were given to 40 key personnel of the internal audit department at ABC Bank requesting them to comment on issues pertaining to the implementation of the RBA methodology, issues such as the benefits, concerns/reservations and suggestions to enhance/expedite the RBA methodology. The survey feedback forms were given to the auditors after an introduction on the risk based auditing methodology was presented to them and before the implementation of the risk based auditing approach. As reflected in the survey feedback, the participants were generally able to appreciate the benefits that can be reaped from the RBA methodology. Among the benefits from the risk based auditing approach voiced by the respondents are:-

(a) risks are identified upfront and classified according to their extremity

Previously, the decision to audit a particular auditable unit is dependent on the criteria such as relevant statutory requirements or whether the area had been audited in the previous 18 months. With the RBA methodology, audits are based on the risks first and the locations where these risks reside. For instance, credit default risk is assessed as one of the major risks faced by ABC Bank. Therefore, the internal auditor decides which are the auditable areas where credit default risk arises and these auditable areas would be incorporated

into the audit plan. Hence, the audit would be more focused on the risks exposed by the particular auditable area. Furthermore, risks identified would be classified according to two factors namely, significance and likelihood. It is justifiable that risks that are assessed as high risks in terms of significance and likelihood are audited. Areas that are considered as low risks may not be audited.

b) **better audit reporting for decision making**

According to the RBA approach, three types of reports will be introduced namely the risk location report, risk category report and group-wide audit report. The risk location report is produced at the end for each audit of a particular risk location. It reports the risks relating to that particular area as well as the manner in which these risks are being managed or mitigated by the management and staff in the auditable area. Subsequently, an assessment is made whether the risks are managed satisfactorily or unsatisfactorily.

The risk category report is produced after all the auditable areas where the risk resides is completed/audited per the financial year's audit plan. In this report, an overall assessment of the identified risk, for example, credit default risk that is exposed by the organization is made, taking into account all the assessments made at the locations where this risk resides.

The group-wide audit report consists of the assessment of all risks identified in the organization and how well these risks are being managed/mitigated. Significant audit findings along with their relevant audit recommendations are included in the report for the Audit Committee of the Board. This report would aid in the preparation of the Statement on Internal Controls as required by the listing

requirements of the Kuala Lumpur Stock Exchange for all listed companies.

These three types of reports are a better form of reporting for risks in relation to its existing controls compared to the previous practice of the internal audit department. Previously, only one type of report is prepared, that is, the audit report for the location. There is no comprehensive review of the overall risks faced by the organization and how these risks are being managed or mitigated based on audit's assessment or perspective. These three types of report depict the risk assessment of the organization both on the micro and macro level. At the micro level, the management of the risk locations is able to conclude whether the risks faced by that particular business units are being managed satisfactorily or unsatisfactorily. At the macro level, the senior level management of the organization would be able to conclude whether the overall risks of the organization are successfully managed/mitigated or vice versa.

c) **optimization of resources as audits are more risk focused and as a result the auditing period may be shortened**

A particular auditable area may be exposed to several and not just one type of risks. For instance, a unit may be exposed to legal risk, employee fraud risk, data integrity, human resources risk apart from credit default risk. Only those risks that are classified as high would be audited in the immediate future. Those risks that are considered as low or medium may be postponed to a future date or not audited at all. In that sense, there is better optimization of resources as the internal audit department acknowledges that it cannot afford to audit all auditable areas in the audit universe and there is a need to manage its limited resources and concentrate on high risks areas. The RBA

approach facilitates the management of resources optimally by placing more importance on auditable areas which are of high risk in nature rather than placing equal importance to all auditable units.

d) a more structured and systematic approach to define, evaluate and mitigate the risk

Although there was some form of risk assessment in the past, the approach differs from one section/unit to another section/unit within the internal audit department. With this RBA approach, consistency in practice within the internal audit department in the implementation of risk-based auditing can be achieved. Furthermore, with the adoption of a single, agreed risk based audit methodology which is understood by all, the implementation of risk based auditing would inevitably be more structured and systematic because the staff from the team member level up to the managerial level understand their role vis-à-vis the methodology.

Notwithstanding that, there was a myriad of concerns or reservations raised by the respondents regarding the implementation of RBA approach. The following sections outline some of the main concerns:

(i) Need For A Monitoring And Evaluation Mechanism

Mechanisms must be in place to periodically assess/evaluate, measure and monitor the effectiveness of the RBA approach and to provide feedback to the audit management. Continuous feedback is required to improve and rectify any shortcomings or weaknesses in the methodology. Proper key performance measurements and monitoring tools need to be in place to measure the accomplishment of the RBA in relation to the overall objective of the RBA approach, that is, to provide value add to the organization.

Furthermore, without proper monitoring, the RBA methodology endorsed by the ACB may go awry and hence, hinder the overall objective of the RBA approach. There should be continuous feedback from either the audit management or the internal auditors in order to improve the methodology, if there are any weaknesses in the RBA methodology. This is because the RBA methodology is a living thing. Where applicable, the methodology should be altered in order to pave a way for a better way of auditing.

(ii) **Need To Communicate the Internal Auditor's Changing Role**

Many auditees may not be aware of the change in the way internal auditors are auditing the risk location. There should be an awareness programme to inform all the auditees of the internal audit department's new auditing approach. The auditees need to be informed of this new audit approach in order to bridge any expectation gap between the auditee and the internal auditor.

(iii) **Internal Auditor's Performance Measurement System Should Be Revised**

The current performance measurement or rewards systems for the internal auditors including head of departments/head of sections need to be revised to ensure that the actual work performed is in line with RBA's objectives. The right performance measurement could be a useful as well as a motivational tool to develop a positive attitude towards the RBA methodology and to spur the internal auditors to achieve the RBA objectives with flying colours. For instance, instead of emphasizing on the time required to complete a particular audit, more emphasis and weightage should be given on the quality of the audit report.

(iv) Need To Change The Internal Auditor's Mindset And Perception

The initial response for any changes is resistance. Therefore, the risk based auditing is definitely a transformation in the way of auditing which the internal audit staff may not be familiar with. Previously, the internal audit staff is used to being provided with the standard audit programmes whereby they are required to based their audit work from. With the RBA approach, the internal audit staff is required to evaluate the risks and to identify the relevant controls in place to mitigate the risks identified. Based on their evaluation, the internal auditors are required to prepare a customized audit programmes in order to test/check the controls in place to ensure whether these controls are operating effectively. Thus, this process requires a lot more thought and analyses which the internal audit staff may object or lack the skills and the competence to do so. Nevertheless, the internal audit staff must be convinced that this is a new way of auditing. Hence, the first thing to change is their current mindset and they must be made to understand that the internal audit profession requires a certain level of competency in the future in order to be considered as a good internal auditor. Furthermore, to drive that change, the key performance measurements for the internal audit staff must be tailored to ensure these changes are introduced albeit gradually.

(v) Training For New Skills Required (for example, interviewing, research and analytical skills)

The RBA approach does not promise an easier way of auditing for the internal auditors. As a matter of fact, new skills are required, for instance, interviewing and analytical skills. These skills are required as internal auditors are required to identify relevant controls in relation to the risks and to assess these controls. These

controls can be in form of hard controls such as design of the controls itself for instance, dual control as well as segregation of duties. Controls can also be in the form of soft controls such as good management oversight, skilled staff/personnel, high integrity of staff performing the work. From such inference, the audit programmes have to be developed to test these controls and subsequently reported to the management accordingly.

(vi) **Deficiency In The Existing Infrastructure**

Currently, the organization structure of the internal audit department is based on 5 main business groups of the financial institution, that is, banking, insurance, finance, investment banking and asset management business groups. Under the RBA approach, consolidation of the report based on risk regardless of which business groups the risk resides is required. Hence, among the issues that need to be addressed is that which section/unit should be responsible to consolidate and to make an overall assessment of the risks regardless of the business groups.

In addition, the RBA approach requires more documentation of the work done from the Group-wide Audit Planning stage to audit testing compared to the traditional approach. Currently, most of the documentation of work done by internal auditors are manually recorded. No audit software is utilized to facilitate capturing of data or information for audit planning purposes as well as for documenting of work done. Therefore, the purchase of a relevant audit software should be considered in order to ensure the successful implementation of the RBA approach.

(vii) Improve Understanding of the RBA approach

The overall understanding of the RBA approach by the internal audit staff especially on the practical applications may still be unclear in order for them to perform the risk-based auditing effectively. Early confusion and lack of understanding of the overall approach is reasonable. However, with proper correction and actual on-the-job training, and relevant coaching, the internal auditors' knowledge of the RBA approach can be re-affirmed and reinforced.