CHAPTER TWO

THE RISK BASED AUDITING APPROACH – DEFINITIONS AND COMPARISONS

2.1 Scope of Internal Audit Function

The scope of internal auditing as specified in the Standards of the Professional Practice of Internal Auditing by the Institute of Internal Auditors (IIA), encompasses the examination and evaluation of the adequacy and effectiveness of the organization's internal control and quality of performance in carrying out assigned responsibilities. The purpose of the review for the adequacy of the system of internal control is to ascertain whether the system established provides reasonable assurance that the organization's objectives and goals will be met efficiently and economically. The purpose of the review for effectiveness of the system of internal control is to ascertain whether the system is functioning as intended. The purpose of the review for the quality of performance is to ascertain whether the organization's objectives and goals have been achieved. The primary objectives of internal controls are to ensure:-

a) the reliability and integrity of information
b) compliance with policies, plans, procedures, laws and regulations
c) the safeguarding of assets
d) the economical and efficient use of resources
e) the accomplishment of established objectives and goals for operations or programs.

In Malaysia, "Best Practices Provision BB VII in Part 2" of the Malaysian Code of Corporate Governance issued by the Kuala Lumpur Stock Exchange states that "The Board should establish an internal audit function. Where an internal audit function does not exist, the Board

should assess whether there are other means of obtaining sufficient assurance of regular review and/or appraisal of the effectiveness of the system of internal controls within the company. The board should explain, in summary, the means that exist for obtaining such assurance of regular review and/or appraisal."

In the banking environment, Bank Negara Malaysia in 1997 issued "Guidelines on Minimum Audit Standards For Internal Auditors of Financial Institutions" (Guidelines). According to the Guidelines, "the core function of an internal audit department is to perform an independent appraisal of the financial institution's activities as a service to the management. The internal audit function plays an important role in helping management to establish and maintain the best possible internal control environment within the financial institution. A sound internal control environment would ensure the financial institution's compliance with legal and regulatory requirements, safeguarding of assets, adequacy of records, prevention or early detection of frauds, material errors and irregularities and efficiency of operation". In addition, the guidelines also stipulate that "the internal auditors should play a participative and consultative role in assisting management to accomplish the financial institution's overall objectives and goals."

2.2 Definition of Risk Based Auditing Approach in Internal Auditing

A risk-based auditing (RBA) approach involves auditing a company and its operations within a risk-filled environment rather than within a system of internal controls. Risk is defined as the exposure to an event or circumstances that may cause loss or damage to a business and its assets, including its employees or its earning capacity. The RBA method assumes that internal controls are not by themselves able to guarantee success in an organization. A good internal control system, starting from

the design of controls to the performance of the controls is not sufficient in mitigating the risks of the business if the internal controls was established to address a risk that is no longer existent. Furthermore, excessive controls established to manage a risk that the organization considered as low/minimal is not cost-effective. Therefore, RBA method involves identifying risks and then testing the relevant internal controls in place as well as evaluating the cost-effectiveness of such internal controls.

Based on the research conducted by James Roth, 2002, for the Institute of Internal Auditors (IIA) Research Foundation, among the major changes facing the internal audit profession is the shift from control or compliance-based auditing approach to risk-based approach. Furthermore, the IIA had slightly revised the definition of internal auditing in 1999 to reflect the following;-

> "internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to educate and improve the effectiveness of risk management, control and governance processes."

The formal term of the paradigm shift from auditing controls, that is, ensuring that all internal controls are in place and performing effectively, to auditing risk, that is, identifying the risks and testing the relevant internal controls used by the organization in managing the risks is known as risk-based auditing. Risk-based auditing (RBA) begins by approaching departmental objectives, risk and adequate controls as interdependent concepts that must function together for success (Rivenbark, William C., 2000). During the past decade,

control models such as COSO[1] and COCO[2] have been a dominant factor in improving internal audit performance and management of organizational risks. Henceforth, risk-based auditing pushes those models a step further and propelling the internal audit profession towards a promising new beginning. Internal auditors who have made the change to RBA would find increased management acceptance and greater integration of the internal audit with other governance elements of risk management.

RBA relies on the COSO sequence with one small upgrade:

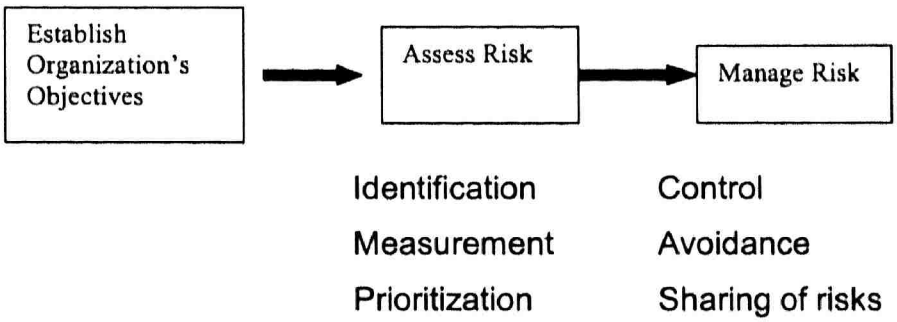

Figure 1: Managing Risks To Achieve Objectives

(Extracted from: McNamee, David, "Risk Based Auditing", Internal Auditor , Aug 1997)

The final step, "Determine Controls Required," is broadened to "Manage Risk." (McNamee, David and Selim, Georges, 1999).

RBA extends and improves the risk assessment model by shifting the audit vision. Risk assessment in internal auditing activity identifies, measures and prioritizes risks so that focus is placed on the auditable areas which have significant risks. In individual audits, risk assessment is used to identify the most important areas within the audit scope. Therefore, instead of looking at the business process in a system of

[1] A system or framework of internal controls defined by the Committee Of Sponsoring Organizations of the Treadway Commission (U.S).

[2] A system or framework of internal controls defined by the Canadian Criteria of Control Board.

internal controls, the internal auditor views the business process in an environment of risk (McNamee, David, 1997).

2.3 Differences In Risk Assessment Approach Between Internal Auditors and External Auditors

For both external and internal auditors, the assessment of risks plays an important role in the planning process. However, the process and factors to be considered by the external auditor and the internal auditor in the risk assessment stage differs from each other. The internal auditor integrates the information gathered during the risk assessment process and uses this information to develop an annual audit plan. The audit plan includes the auditable units that will be examined during the year, when the particular auditable unit will be audited and the approximate timeline required for that particular audit. On the other hand, the external auditor uses the risk assessment process to determine the nature, timing and extent of substantive testing to be performed to enable them to express an opinion on the overall financial statements of a particular organization.

2.4 Motivations For Changing The Traditional Auditing Approach

When controls are the central theme of the internal audit, more and more audit reports and recommendations are generated for improving and strengthening internal controls. Over time, layer upon layer of controls are built up, creating an "organizational plaque." These excessive layers slow down business processes (McNamee, David and Selim, Georges, 1999).

Instead of identifying and testing controls, the auditor will identify risk and test the ways management mitigates these risks. The majority of risk mitigation techniques will still involve controls, but the auditor will

test "how well are these risks being managed?" rather than "are the controls over this risk adequate and effective?" (McNamee, David, 1997).

Despite the advantages, a recent study by the IIA's Austin Chapter (U.S) shows that at least one-third of all audit groups fail to use RBA. Other less formal research seems to confirm this surprising finding and suggests that the reasons may be several, as follows:

- "risk concepts are not clearly understood
- auditors believe that risk assessment requires specialized knowledge or software
- there is too little time for planning – the continuous "do" loop,
- many internal audit shops feel their operation is too small to use planning tools
- internal auditors feel compliance/inspection/financial auditing does not fit with risk" (McNamee, David, 1997)

In the past, some auditees have criticized internal auditing for being too focused on historical records. "Driving the car by looking in the rear view mirror" was one of the more telling metaphors. This metaphor characterizes the internal auditor as one who renders advice and recommendations based on examination of the historical transaction records and the historical operation of the internal control system. In order to extend more value to the organization, internal auditors should shift their focus from being past-oriented, that is focusing on compliance of internal control to a future oriented audit, that is, focusing on risks and the internal controls in place in managing/mitigating such risks. Each control added to the system costs more resources to operate. If the internal auditors continue to audit and recommend new and strengthened controls without removing any, the weight of these controls will drag the business process down (McNamee, David, 1997)

According to a paper titled *Internal Audit in Banks and supervisor's relationship with auditors,* by the Basel[3] Committee on Banking Supervision "the scope of internal audit should include examination and evaluation of the appropriateness and effectiveness of the internal control system and of the manner in which assigned responsibilities are fulfilled. In many respects, this represents a risk analysis on the bank's internal control system. The audit plan is based on a methodical control risk assessment. A control risk assessment documents the internal auditor's understanding of the institution's significant activities and their associated risks. The management of the internal audit department should establish principles of the risk assessment methodology in writing and regularly update them to reflect changes to the system of internal control or work process and to incorporate new lines of business. The risk analysis examines all of the bank's activities and entities, and the complete internal control system within the organization of the bank. On the basis of the results of the risk analysis, an audit plan for several years is established, taking into account the degree of risk inherent in the activities."

2.5 Differences Between The Traditional Auditing Approach and RBA Approach

Table 1 summarizes the differences between the traditional auditing approach and RBA approach. These differences are discussed in the following sections.

[3] The Basel Committee was established by the central bank Governors of the Group of Ten countries at the end of 1974. The Committee does not possess any formal supranational supervisory authority, and its conclusions do not and never intended to, have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements – statutory or otherwise – which are suited to their own national systems. In this way, the Committee encourages convergence towards common approaches and common standards without attempting detailed harmonisation of member countries' supervisory techniques.

CHARACTERISTICS	OLD PARADIGM	NEW PARADIGM
Internal Audit Focus	Internal Control	Business Risk
Internal Audit Response	Reactive, after-the-fact, discontinuous, observers of strategic planning initiatives	Coactive, real-time, continuous monitoring, participants in strategic plans
Risk Assessment	Risk Factors	Scenario Planning
Internal Audit Tests	Important Controls	Important Risks
Internal Audit Methods	Emphasis on the completeness of detail controls testing	Emphasis on the significance of broad business risks covered
Internal Audit Recommendations	Internal Control : • Strengthened • Cost-Benefit • Efficient/Effective	Risk Management : • Avoid/Diversify Risk • Share/Transfer Risk • Control/Accept Risk
Internal Audit Reports	Addressing the functional controls	Addressing the process risk
Internal Audit Role in The Organization	Independent Appraisal Function	Integrated Risk Management and Corporate Governance

(Extracted from: Risk Management: Changing The Internal Auditor's Paradigm, McNamee, David and Selim, M. Georges)

Table 1 : Differences Between the Old and the New Paradigm

2.5.1 Internal Audit Focus

In the past, internal auditors focused on controls in the business process resulting in the auditors being buried in the details of the past and limiting the value of any information derived. Concentrating on internal controls causes the internal auditors to focus on establishing whether the internal controls were operating effectively and whether there were non-compliances of these controls in the past as well as during the period of

audit. On the other hand, RBA approach forces the internal auditor to look at the risks facing the organization. Internal auditors typically examine the control activities designed at some previous time to deal with issues that may have been long forgotten. This means that the internal auditors are examining activities that may or may not be relevant to prevailing/current business risks. However, in the RBA approach, the internal auditor focuses on risks in the present and future transactions, thereby working above the level of details and dealing with obstacles obstructing the success of an organization. The information derived from such exploration commands a great value to the management in the running of a business concern effectively and efficiently as well as economically.

2.5.2 **Internal Audit Response**

Under the traditional audit approach, the internal audit response is re-active (looking into the past and the present). However, under the RBA approach, the internal auditors are more co-active. This means that the auditee is seen as a partner or an ally and both parties will be viewing the business from the same perspective, namely management of risk. Furthermore, under the traditional audit approach, the audit on a particular auditable activity is discontinuous, that is, the auditor will only revisit the auditee based on audit cycles for instance, on a yearly basis. On the other hand, under the RBA approach, the internal auditor will revisit the auditee depending on the risks prevalent. For instance, if the risks assessed at a particular auditable area are considered extreme in the terms of significance and likelihood of occurrence, more frequent visits will be scheduled. For example, the internal auditors will visit an auditee with higher risks every half-yearly whereas an auditee with low to medium risks, the visits would be less frequent. In addition, the internal auditor will report to the Audit Committee of the Board on a continual, periodical basis on how the risks are being managed and controlled at the respective risk

locations. Finally, under the traditional audit approach, the internal auditors are merely observers of the strategic planning initiatives of the management and will report to the Board on the status of implementation of the initiatives undertaken. However, under the RBA approach, the internal auditor also participates in the formation of strategic plans of the organization. For instance, internal auditor could provide input/insights to management by recommending appropriate performance measures/reward systems in order to ensure successful implementation of strategic plan of the organization. Under the RBA approach, the auditors would consider the performance measures used by other competitors in the industry or industry players and whether such performance measures are also being used by the organization to measure its performance vis-à-vis the competitors.

2.5.3 **Risk Assessment**

Under the RBA approach, scenario planning would provide a better macro risk assessment tool in times of significant change, such as merger, acquisition and divestiture of major business units. Scenarios are based on possible, credible and relevant hypothesis. In order to build a possible, credible and relevant hypothesis, certain building blocks/factors need to be considered. The factors or building blocks to be considered are such as drivers of change, key uncertainties, basic trends and how these factors interact with each other to materialize into multiple scenarios that the organization would encounter in the near, plausible future.

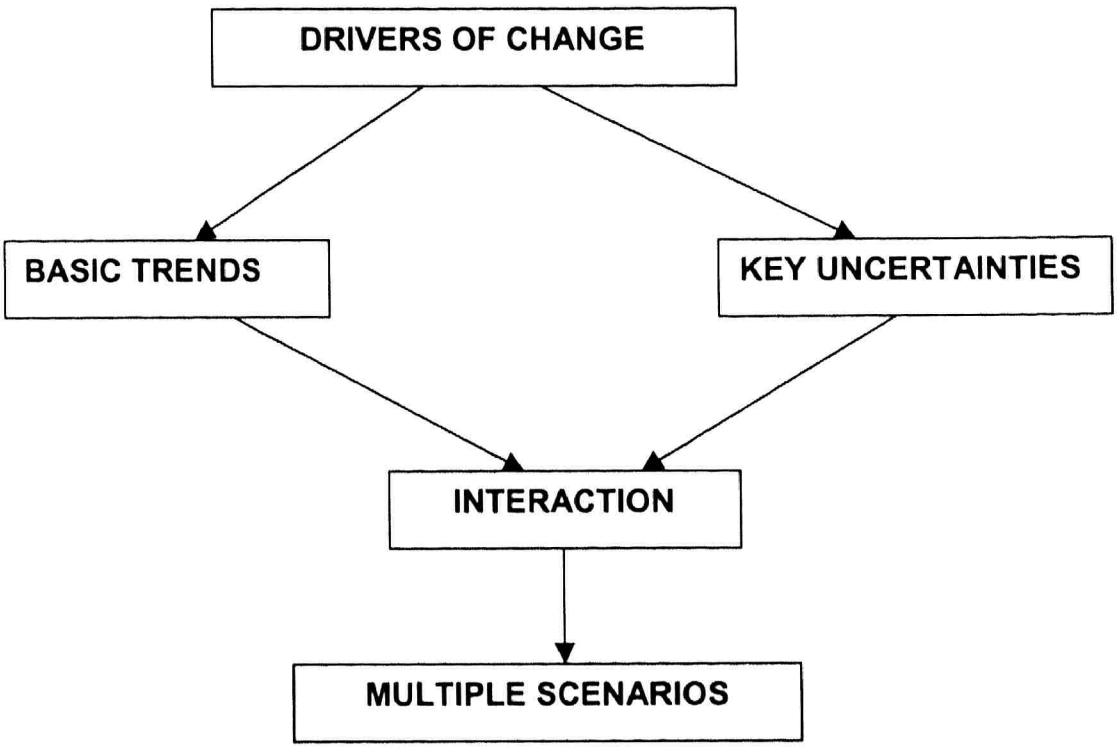

Figure 2 : Building Blocks for Strategic Planning Scenarios

(Extracted from: Shoemaker, Paul J. H., "Scenario Planning : A Tool for Strategic Thinking , "*Sloan Management Review*, Winter 1995)

Scenario planning includes and combines each of the three factors under risk assessment:

a) by thinking of possible scenarios affecting the business process, the internal auditor will be able to understand the business process better. For example, in the event of market liberalization in the financial markets, the internal auditor could visualize the challenges that the organization would face. Furthermore, the internal auditor could also evaluate whether the organization could withstand the force of such new competitive threats based on the internal auditors' understanding of the current financial situation as well business conditions and operating environment of the organization.

b) Scenario planning provides the framework for intellectual discourse between management and auditors. Through scenario planning, the auditors will be able to have a better discussion with the management because ultimately, management is interested in the risks affecting its business. For instance, auditors can initiate a discussion by inquiring the management on the current and potential risks that is currently faced by management. The management of a particular business unit may quote customer satisfaction as its major risk. The internal auditor could then stimulate the conversation by inquiring the manager concerned on the reasons or situations that resulted in such risks to be his current priority/concern.

c) Scenario planning is also a means to open up the imagination about other significant risk potential. Through the interviews with management, the auditor could also bring up other possible risks facing the management. For instance, apart from customer satisfaction risks, the internal auditor could also derive other risks being faced by the organization such as human resource risks in the form of poor or lack of training provided to staff in terms of customer service.

Furthermore, scenario planning has a special use in micro risk assessment in the areas of fraud, crisis management and catastrophe. By using fraud risk scenarios, for instance, the internal auditor can actually identify the sources of fraud before it happens – and then change the controls or system design to change the fraud risk potential.

2.5.4 Internal Audit Tests And Methods

Under the traditional approach, the audit tests are designed to test the controls established in the organization with the emphasis on determining whether these controls are being complied by staff and whether non-compliances are rectified accordingly. On the other hand, for RBA approach, the internal auditor will test whether there are appropriate controls to mitigate a particular risk and whether such controls, if available, are operating effectively. Emphasis is given on significant broad business risks affecting a business entity.

2.5.5. Internal Audit Recommendations

Under the traditional approach, the recommendations accompanying the audit findings promulgates on how the internal controls system of a particular process can be further strengthened. This is done after the internal auditor considers its cost-benefit analysis as well as whether the controls in place are operating effectively and efficiently. On the other hand, under the RBA approach, audit recommendations are in line with risk management principles in that it is impossible to avoid risks completely and economically. The management will have to decide on which risks to accept or reject in the organization. Consequently, alternatives/recommendations must be established or designed in order to control the accepted risks.

2.5.6 Internal Audit Reports

Previously, the internal auditor will report on the functional controls of the processes audited, that is, whether these controls are efficient and effective. Under the RBA approach, the audit report discuss on whether all the risks relating to a particular business process for instance

transferring of funds via electronic devices are being addressed by management by establishing appropriate controls to mitigate the prevailing and future risks.

2.5.7 Internal Audit Role In The Organization

Under the traditional auditing approach, the internal auditors' role in the organization serves as an independent appraisal function. However, under the RBA approach, the internal audit's roles/functions are intertwined and form part of the integrated risk management function and corporate governance of the organization. For instance, the chief internal auditor could be involved in the risk management process of the organization through establishing a common language and risk framework to discuss risk with senior management. Secondly, the organization's strategic plans are used to derive elements of the audit universe. The audit universe of the internal audit department is the sum of all the auditable units of the organization. In that way, the audit universe contains the essential elements to support the overall business plan of the company. Table 2 is an illustration on how the strategic plans of an organization can impact on the audit universe of an internal audit department.

Strategic Plans	**Strategic Plans Goals**	**Audit Universe**
To become leading provider of financial services.	To provide more delivery channels in terms of customer service such as internet banking services, self-service terminals, 24-hour ATM services etc.	Internet Banking Services (Risk Location : Electronic Banking Division)
To penetrate international	To open new foreign branches/ representative	Budgeting and planning function.

Strategic Plans	Strategic Plans Goals	Audit Universe
markets.	offices.	(Risk Location: International Banking Division)

Table 2: The Relationship Between Strategic Plans And Audit Universe

As described from the above paragraphs, RBA addresses some of the important questions that controls-based auditing leaves unanswered. RBA is a major step toward an improved internal audit performance and organizational risk management. Internal auditors who have made the change to RBA have found increased management acceptance and greater integration of the internal audit with other governance elements of risk management.

Differences between risk-based auditing approach and traditional auditing approach are also illustrated in Table 3:

FROM	TO
Fragmented	Continuous
Negative	Positive
Reactive	Proactive
Cost-based	Value-driven
Compliance & rotational focus	Risk focus
Mechanical	Judgmental

Table 3 : Differences Between The Traditional Auditing Approach And Risk Based Auditing Approach

Another look at the approach adopted in the risk-focused examinations conducted by renowned financial institutions regulators such as the Federal

Reserve Bank of New York (FRBNY) revealed that, historically, examinations relied significantly on transaction-testing procedures when assessing the condition of a bank and verifying its adherence to internal policies and procedures controls. However, the thrust nowadays for the FRBNY is towards risk management process. Based on the FRBNY's Commercial Bank's Examination Manual, it was espoused that when the examiners evaluates the quality of risk management, the examiners would consider findings relating to the following elements of a sound risk management system:-

1. Active board and senior management oversight
2. Adequate policies, procedures and limits
3. Adequate risk measurement, monitoring and management information systems
4. Comprehensive internal controls

A comparison between the traditional approach (Traditional Bank Examinations) and the risk-based approach (Risk-Focused Supervision) as espoused by the Federal Reserve Bank is shown in Table 4.

Traditional Bank Examinations	**Risk-Focused Supervision**
Supervisory process is focused on a single point in time and is rarely continuous unless there is a crisis	Supervisory process is continuous and is more tuned to market developments.
Examinations are generally staffed locally.	Institutions are assigned designated supervisory teams. The teams are supplemented with specialists, who may be drawn from across the Federal Reserve System
Significant emphasis is placed on valuation of assets	Focus is on risk management processes and control systems

Traditional Bank Examinations	Risk-Focused Supervision
Dialogue with management is mostly related to examination findings unless there is a crisis	There is more frequent communication with senior management
	Supervisory process includes more interaction with line management of business activities and risks
	Program includes business lines and functional reviews that incorporate identification of best practices.

(Extracted from the FRB's Commercial Bank Examination Manual)

Table 4 : Comparison Between Traditional Bank Examinations And Risk-focused Supervisions By The Federal Reserve Bank