EMERGING ISSUES IN RISK AND SOUND RISK MANAGEMENT

By
Niroshana Seneviratne

Objective of Internal Audit

The main aim of any activity in an organisation should be to achieve the objectives of the organisation. Thus, the main aim of internal auditing is to assist the organisation to achieve its objectives. Be it "enhance shareholder value" or "effective distribution of tsunami relief", same would be the aim of internal audit.

Achievement of organizations' objectives are hindered by risk. In simple terms, a risk is a set of circumstances that hinder the achievement of objectives. Risk could be avoided, transferred, retained or mitigated. It is the responsibility of the management of an organisation to manage risk to gain from the opportunities while mitigating risk to minimise the exposure.

Risk management is a term widely used, and organizations assign the task to a "Risk Manager" who constantly monitors and manages risk. Theoretically, since managers own risks, they must "manage" them. That accountability cannot be passed to a third party. Risk Managers assist the organisation to identify its risks, run risk workshops, coach staff in risk management and set "best practice standards".

Internal Controls

Internal control system is a process that Risk Managers use to mitigate risk. In general terms – it effects controls, from within an organisation, to safeguard its assets.

Definition

" The whole system of controls financial and otherwise, established by the management in order to carry on the business of the enterprise in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records."

UK Auditing Guidelines

Responsibility to implement effective internal controls is with the Management of the organisation. Internal Auditor is responsible to independently report that internal controls are operating effectively and whether the controls are adequate and are being complied with by the respective officers. Recent financial scandals have re-emphasised the need for this type of independent opinion.

Over the past few years, there have been major company failures due to financial irregularities.

This has inevitably led to several countries introducing regulations to tighten internal controls within companies. The primary regulations in the U.K. come from the London Stock Exchange Combined Code, backed up by the Turnbull Committee guidance. In the U.S., the Sarbanes-Oxley act, the legislation, is supported by standards from the Public Company Accounting Oversight Board (PCAOB).

In Sri Lanka "The Corporate Governance Code", a voluntary code, issued by the Institute of Chartered Accountants of Sri Lanka emphasizes the importance of implementing an effective internal control system within an organisation.

Internal Audit

Definition

"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 evaluate and improve the effectiveness of risk management, control, and governance processes"

Institute of Internal Auditors

As per the above definition, it is a consultative activity designed to add value to an organisation. It is imperative that the internal auditor, among other qualities, practises independence, integrity and objectivity in all assignments, even after the assignment is over.
Not only that he practises those qualities, but more importantly he should appear to be practising, to secure the trust and the acceptance of the auditee.

Risk Based Approach

Traditionally, the internal audit has been a post event review that depended mostly on substantive testing which was referred to as Substantive Approach. Since of late, auditors reviewed their task in the context of a business system which is referred to as the Systems Approach.

Diagram 1

Auditors generally evaluate Audit Risk which is a combination of Inherent Risk (risks that stem from the industry, legal framework of the business etc), Control Risk (risks from controls within the organization, not preventing or detecting errors or frauds) and Detection Risk (risk of audit procedure not preventing or detecting an error or fraud).

Audit Risk = Inherent Risk X Control Risk X Detection Risk

As a solution to allocate its limited resources, mostly to prioritise audits that have been lined up, auditors now increasingly adopt a Risk Based Approach. The risk based approach is more focussed , effective , efficient and economical. The risk based approach goes beyond the traditional horizon of audit risk and evaluate in detail the operational risk, market risk, credit risk, legal risk etc attached to each sub process in a business.

Risk Based Approach - Transformation and Benefits
Table 1

Audit process	Risk-based auditing	Previous methodology
Audit Coverage	All activities of the business	Primarily financial areas but also involving compliance with laws, regulations and "operations"
Audit objective	Provide assurance that risks are being mitigated to acceptable levels	Confirm internal controls are operating. Improve efficiency
Annual plan	Audits directed at high risks	Cyclical plan of audits, not necessarily dependent on risk levels
Involvement of the rest of the organisation	Involved at all stages of planning and the audit, since they own the risks and must provide assurance to the stakeholders	Minimal. May approve the audit plan and be involved at the end of an audit to agree the points found
Staff plan	Several audits allocated to one or more staff at any one time	One audit allocated to one or more staff
Time budgets	Difficult to set. May be a first-time audit, or one where systems have changed	Easy to set – since the audit has usually been done before
Fieldwork	Ensures the organisation has identified all its risks, and is controlling them	Based on a set work programme, where there may be no clear objective set, just test to carry out
Testing	Similar tests as used at present but aimed at confirming that important controls are operating	Confirms the operation of controls – but may not prioritise these in order of importance. May also be directed towards finding errors, however immaterial.
Report	Assures management that its risks are being mitigated to acceptable levels; reports if they are not	Confirms internal controls are operating and reports
Annual report to the "board"	Provides assurance that the significant risks across the organisation are being mitigated to acceptable levels and reports where they are not. Can give an	Confirms that the audit plan has been completed and highlights controls not operating. Cannot give any indication as to the proportion of significant risks covered

	indication as to the proportion of risks covered	
Staffing	Self-motivated, experienced staff used to working with senior management. May be specialists who are not accountants and may be seconded.	Usually accountants and career internal auditors

Steps in Risk Based Approach

a) Identify types of risk that the business is exposed.
b) Assess the impact on each business process
c) Quantify the potential impact
d) Risk based audit year plan
e) Planning the audit
f) Fieldwork
g) Audit finalisation
h) Report

a) Identify Risk Types

The organisation depending on the business and the industry may be subject to various types of risk. Risk is the possibility of losses, financial or otherwise or serious negative deviations from forecasted position.

Banks specially are exposed to credit, market and operational risk, which if carefully managed, should not only prevent any financial losses, but also would provide opportunities for new or greater business which would result in significant returns. Generally the magnitude of risk is high in the business of banking compared to non banking sector. The banking and finance sector is highly regulated world over due to such volatility. The regulatory framework exposes the bank to legal risk that includes reputational risk.

In a risk management perspective, risk managers while understanding the positive correlation between risk and return, minimize some risks, while consciously retaining certain exposures to gain returns.

In an audit perspective, risks are assessed for their vulnerabilities and possible impact on the business processes.

b) Assess the Impact on Business Processes

All the functions of the bank be it Treasury, Trade Finance ,Corporate Banking , Branches or Central Processing, should be split into auditable chunks or processes Examples of possible sub-processes within two processes in Central Processing that could be audited,

- Outward Cheque Clearing

- Scrutinizing and crossing
- Sorting and Stamping
- Posting and Authorisation
- Encoding and Batching
- Balancing and Reconciliation

- Pay-order

- Request processing
- Posting and authorization

- Issues
- Handling blank stock
- Reconciliation
- Stale pay-orders
- Cancellations

Each sub process then should closely be evaluated to identify the different types of vulnerabilities that could be exploited. The severity of the impact on the sub process, probability of vulnerability being exploited and mitigating controls are evaluated critically to assess the overall risk attached to each sub process.

Table 2
Format for Impact Assessment

Vulnerability	Impact	Probability	Mitigating Controls

The vulnerability could broadly be evaluated in the context of ,

- Operational Risk

Risks that arise from information systems, procedures or inadequate controls such as errors, omissions, delays, inaccurate information etc.

- Credit Risk

Possibility of a loss in case of non payment by a customer that may result in from inadequate verification of credit worthiness, excessive credit limits, failure to perform as agreed etc.

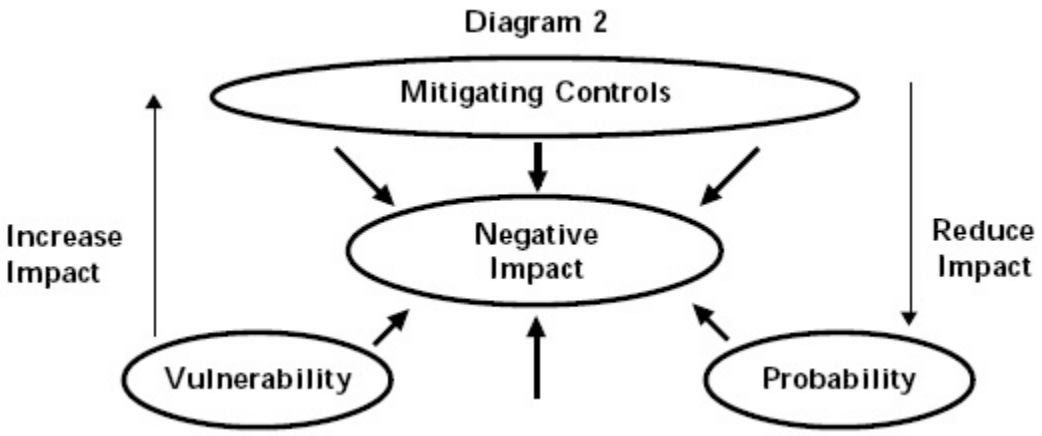
- Market Risk

Risks associated with changes in the market outside the control of the organization such as exchange and interest rate fluctuations.

- Legal or Reputational Risk

Risks associated with violation of laws, regulations and incomplete legal documentation etc.

The vulnerability, together with the probability of occurrence may have a negative impact on the business process under scrutiny and mitigating preventive or detective controls may reduce the impact.



c . Quantify the Potential Impact

The risk factors and most of their impact on the business would be qualitative and quantification and may be complex. To eliminate subjectivity to an extent and to measure the impact on a comparative basis, a standard risk score could be assigned to each risk element attached to each sub-process that has been identified.

Steps in Risk Scoring

- Identify vulnerabilities attached to each sub process

- Evaluate the impact on the business considering the mitigating controls. For simplicity assign a score out of 3 (3 - High risk, 2 - Medium risk & 1 - Low risk)

- Evaluate the likelihood of Occurrence (Probability) and assign a score out of 3 (3 - High likelihood, 2 - Medium likelihood & 1- low likelihood)

Both impact and likelihood of occurrence are manageable if the mitigating controls are effectively complied with. Table 3, below indicates few vulnerabilities attached to Information system of an organisation.

Vulnerability 1 - The likelihood of virus attacks to any organisation is high.

However if the policies are in place and preventive measures such as virus guards, removal of disk drives from PCs etc are being effectively complied with, the probability of the attacks could be reduced. Therefore, marked as medium (2).

Similarly, the impact could be minimised if the corrective or backup arrangements are effectively in place. Assuming that no effective backup arrangement is in place, the risk is assessed as high (3)

Vulnerability 2 - If the organisation is dependent on head of IT and there is no second line

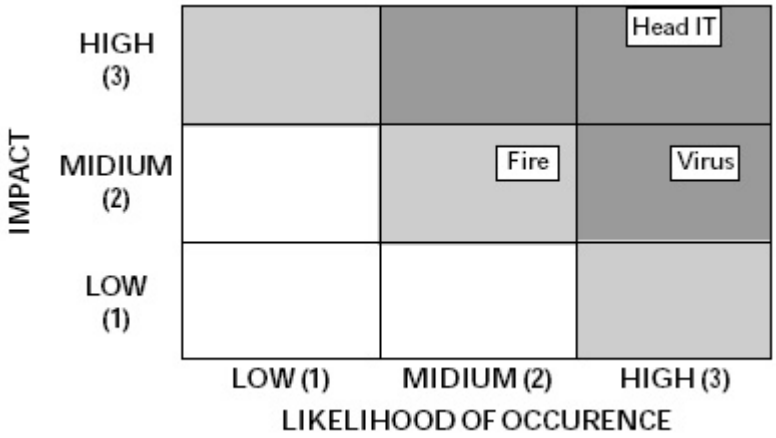
groomed, the person becomes indispensable. Both the impact and likelihood have been assessed as high risk (3)

Table 3
Vulnerability Assessment

Vulnerability (Risk Driver)	Impact after considering mitigating controls	Likelihood of Occurrence (Probability)
1. Virus attack on Information System	2	3
2. Loss of key IT personnel	3	3
3. Disruption to IT system by fire	2	2

The above risk drivers could be plotted on a simple graph considering Likelihood of Occurrence (Probability) as the horizontal axis and Impact from the risk driver as the vertical axis. The areas with dark shading, indicate high risk that need managements' as well as auditors' immediate attention: those lightly shaded are next in priority for such attention; whereas the areas not shaded require the least priority.

Diagram 3
Impact Probability Matrix



In the context of managing operational risk in the perspective of BASEL II, the "Impact Probability Grid" would be immensely useful. The Risk Manager, through series of brain storming sessions, should "Risk Rate" all the processes and propose conscious changes to push them from darker cages to lighter ones.

Processes up to step "c" is common to both Risk Managers and Auditors, steps "d" onwards applies to Internal Auditors.

d. Risk Based Annual Audit Plan

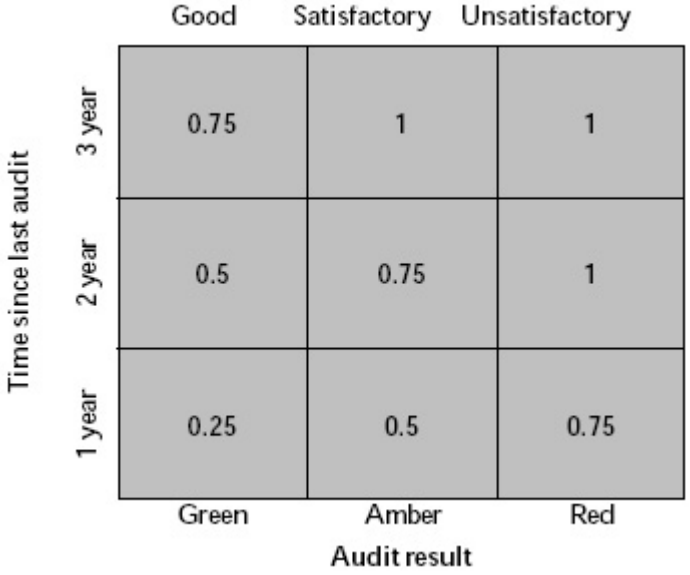
Auditor should necessarily be guided by a proper annual audit plan that has been scheduled after considering,

- The risk score (significance)
- Time since the last audit

- The results of the audit or the audit rating

The total Risk Score is derived from the **Impact and Probability** (Diagram 3) **and time since the last audit and Rating** (Diagram 4) **.**

Diagram 4
Audit Due Result Matrix



Audit reports, depending on the significance of findings could be rated as Good, Satisfactory or Unsatisfactory. Similarly the duration since last audit could be 1 to 3 years. The chart will indicate the appropriate score.

For example, appropriate value, if the previous audit performed 2 years ago had been rated satisfactory, would be 0.75.

The total score for audit planning purposes could be arrived as follows.

Total Risk Score = Impact X Probability X Previous Audit Score

Eg: Audit of Virus Policy

Assuming two years since the last audit which was rated satisfactory, the total Risk Score could be calculated as follows.

Total Risk Score = Impact(2) X Probability (3) X (Diagram 4) 0.75
Total Risk Score = 4.5

As given in Table 4, depending on the final risk score for each sub process, the audit frequency or the audit cycle is decided, based on which the annual audit plan is drawn prioritising audits that expose the company to significant risks.

Table 4
Audit Cycle Chart

Audit Cycle	Risk Score (1-9)
Every Six Months	6.75 and above
Every one year	4.5 to 6.75
Every one and half years	3 to 4.5
Two years	Below 3

Higher the risk score, shorter would be the audit cycle.

As per table 4, since the Virus Policy Audit has a overall risk score of 4.5, next audit is due within this year.

Table 5
Annual Audit Plan

	Audit Area	Impact	Probability	Last Audit	Total Risk	Audit	Jan	Feb	Mar	Apr	May	Jun
		Score	Score	Score	Score	Cycle						
1	Audit of Virus Policy	2	3	0.75	4.5	1 year			P			
2	Audit of IT Infrastructure (Personnel)	3	3	0.5	3	1.5 years						
3	Audit of IT Environment (Fire)	2	2	0.5	2	2 years						

e. Planning the Audit

Understanding the Business

Audit planning is of paramount importance to perform an audit effectively that would involve more than 60% of the total time allocated for the audit. It is the primary information gathering stage to understand the scope of the audit to develop audit objectives.

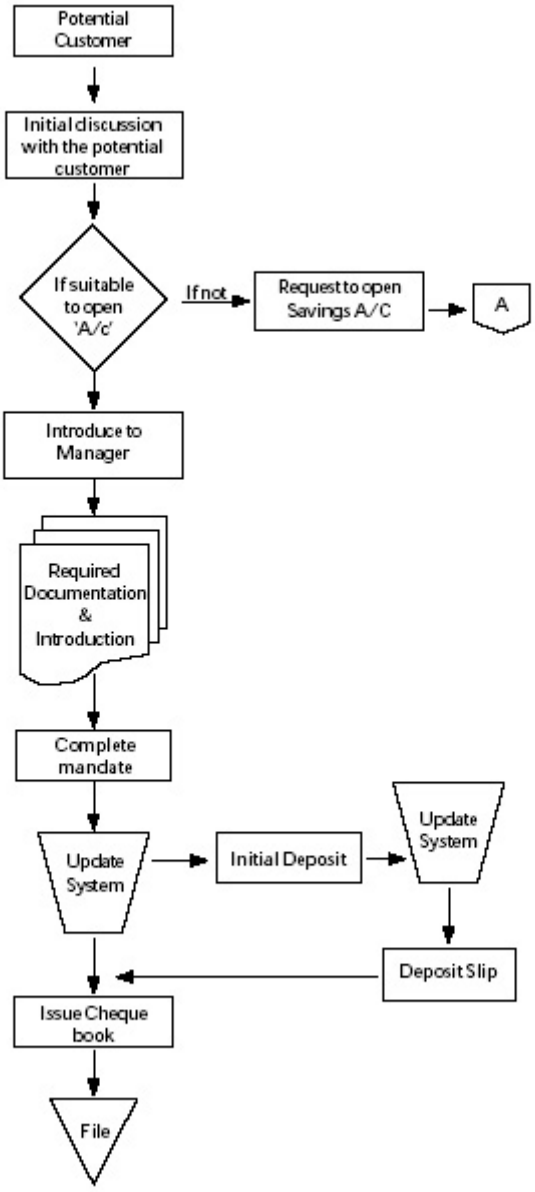
Once the auditor is clear of the audit scope, it is required to understand the relevant business process. The auditor should visit the process; through continuous dialog with the business lines, document the process flow. The process mapping charts so documented should be tested for accuracy through ‘walk through’ tests.

The auditor should keep in mind that the exercise is to document what is being practised at the business line and not what should have been practised. Walking through the documented process, few sample transactions would enable auditor to ensure what he has documented, is in fact being practised by the business line.

As a value addition to business line, it is advisable to get the business line involved in the process mapping and once completed, get their sign-off as a confirmation.

Diagram 5 below indicates a simple process flow diagram for Opening a Current Account (“C/A”).

Diagram 5



Evaluate Control Environment

The documented process flow should then be critically evaluated to identify process gaps that would make way for frauds and errors. The evaluation could be effectively carried out by formulating “What could go wrong” questions and finding answers to such questions.

Brain storming sessions would be more effective and appropriate in evaluating business processes flows.

Develop Audit Programs

An audit program indicates the audit process that would be followed to achieve audit objectives. The documented process when compared against the laid down procedures would highlight

deviations from procedure, which require auditor's special attention. In developing audit programs, auditors should focus more on the gaps identified through the above process.

Allocate Resources

Based on the scope, risk rating , extent of coverage, audit programs etc , the audit resources would be allocated. Unlike traditional auditing , in risk based auditing, an auditor may be assigned more than one audit that he should perform simultaneously to save time and efforts.

f. Audit Field Work

Auditor would carry out audit tests according to the audit program that the team had developed. Auditor would now have an overall view of the business, gaps in the process with the relevant exposure, deviations from the procedures, more over the required background to converse with the auditee who would appreciate the business knowledge of the auditor. Auditors' recommendations would now be more practical and acceptable to the business line.

The auditor would collect only the essential evidence, as the likelihood of auditee challenging the findings would be minimal.

g. Audit Finalization

Clarification should be obtained at field level stage through continuous dialog with the business line. The practicality of the recommendations also should be ensured during the finalisation stage. All audit findings should be discussed with the respective line head before being included in the final report.

Each finding should be rated with an appropriate risk indicator to attract the readers' attention.

Low Risk (unshaded)

The solutions to which may lead to improvement in the quality and/or efficiency of the organizational entity or process being audited. Risks are limited. Routine management attention is warranted.

Medium Risk (lightly shaded)

Those that may lead to (1) financial losses; (2) loss of controls within the organizational entity or process being audited; (3) reputational damage; and/or (4) adverse regulatory impact. Timely management attention is warranted.

High Risk (darkly shaded)

Serious audit findings that may lead to: (1) substantial losses, possibly in conjunction with other weaknesses in the control framework of the organizational entity or process being audited; (2)

serious violation of corporate strategies, policies or values; (3) serious reputational damage; and/or (4) significant adverse regulatory impact. Immediate management attention is required.

h. Audit Report

Audit Findings after discussion should be recorded and forwarded for management comments. More importantly, the findings noted should be,

- Objective oriented and relevant to the assignment
- Accurate in all respect
- Supported by evidence
- Reported promptly

Auditor should ensure that the management comments include an action date which the auditor would follow-up until implementation.

The audit report should appropriately rated, based on the materiality of the findings.

Good	→	Risks and processes are properly controlled
Satisfactory	→	Minor audit findings. Risks and processes are adequately controlled
Unsatisfactory	→	Serious audit findings; risks and processes are inadequately controlled

The final audit rating could be directly linked to business line managers' performance appraisals. When business managers are appraised, obtaining a"Good" audit rating could be included as an objective which could be assessed against the final rating of the audit.

Conclusion

The benefits of risk-based auditing are considerable:

- Risk-based auditing is a simple concept. There is no need for a complex definition of internal control, or internal auditing, and it involves the whole organisation and its processes – so no need to define which functions internal auditing should involve. It should involve all of them.
- Alongside this simplicity, there is a unity. The recommendations made can be traced back

through controls, risks and processes to the organisation's objectives. Similarly, we can easily demonstrate what proportion of significant risks we have audited, and the results, to provide assurance to the board about the "effectiveness of the company's system of internal control" .

- The organisation buys in to the audit process. As it has to be closely involved in the process and should be able to clearly see the benefits of the Auditor's output, it is far more likely to support the audit work, as opposed to treating it like an unwanted imposition.

- The work is more challenging and interesting to staff. They have to work in non-finance areas, with staff who may be seconded in for the audit. There is no handle-turning of work programmes, without really understanding why the test is being done.

- Risk-based auditing is more efficient, because it directs audits at the high risk areas, as opposed to financial areas, which may not represent such a great risk.

- Auditor can rank recommendations, to provide the greatest value added in terms of the risks mitigated.

Fundamentally, the internal audit function is now much more part of the organisation and less introspective. It involves the organisation more in the audit process and produces recommendations which contribute to its objectives. At the same time it has to be careful not to lose its independence and objectivity, as a result of getting closer to the operations.

Unlike in the past, it is increasingly important that the auditor takes all efforts to make the business line invite the auditor to contribute in improving its processes.

It is risk based auditing that would help the auditor achieve this objective.

References :

Tone at the Top, "Those at the top applauds value of Internal Auditing", IIA, Special edition , April 2005

Tone at the Top, "Call for Character and Integrity", IIA, June 2005
IIA Magazine, "Risk in Auditors perspective", IIA, February 2005

www.whistleblower.org
www.isaca.org

Niroshana Seneviratne

Niroshana Seneviratne is a Fellow of the Institute of Chartered Accountants of SL, Associate of the Institute of Bankers, Certified Information Systems Auditor, (CISA) USA and holds a Masters Degree in Management from University of Sri Jayawardenapura. Currently attached to NDB Group as an Assistant Vice President, Head - Group Internal Audit. He is a Chief Examiner at Institute of Bankers of SL and a lecturer in Finance and Audit.