Guide on
Risk-based Internal Audit

Committee on Internal Audit

The Institute of Chartered Accountants of India

(Set up under an Act of Parliament)

Appendix I

Model Process for Assessing and Evaluating Risks

Steps in Risk Assessment

1. Activities in risk assessment can be put in three processes, *viz.*
   - Risk identification.
   - Risk estimation.
   - Risk evaluation.

Risk Assessment Tools

2. Following are some of the popular analytical methods used during risk assessment:
   - Market survey.
   - Dependency modeling.
   - SWOT (Strength, Weakness, Opportunity and Threat) analysis.
   - Event tree analysis.
   - BPEST (Business, Political, Economical, Social and Technological) analysis.

- Fault tree analysis (Root Cause Analysis).
- FMEA (Failure Mode and Effect Analysis).

Risk Identification

3. This is the start point for all risk assessment initiatives. As mentioned earlier all organizations are exposed to varieties of threats and uncertainties which impact the objectives for which they have been established. It is essential that the risk identification process be planned and activities within streamlined. This process should ideally cover all risks and scenarios to which an organization is exposed to during the normal course of its business and also the various business activities which are a source of these risks.

4. Some of the business activities, which are a source of risk, are:

- **Strategic** - These concern the long-term strategic objectives of the organization. They can be affected by capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.
- **Operational** - These concern the day-to-day issues that the organization is confronted with as it strives to deliver it strategic objectives.
- **Financial** - These concern the effective management and control of the finances of the organization and are affected by external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.
- **Human Resources and Knowledge Management** - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External risks include the unauthorized use or abuse of intellectual property. Internal risk could be loss of key staff.
- **Compliance** - These concern issues as health and safety, environmental, trade regulations, consumer protection, data protection, employment practices and regulatory issues.
- **Fraud** - All large organizations are exposed to fraud risks. Also various regulatory requirement as Clause 49 require organizations to have sound fraud control mechanisms in place

5. What is the best way to identify these risks? Whether it should be identified by people within the organization? Or external resources who specialize in these areas? Or a blend of both internal and external specialists? Who are the best resources internally to perform risk identification?

   Once again there is no standard practice or guideline which is followed. This decision would depend upon the management, expertise of internal resources, etc. Generally Internal Auditors are considered to be the appropriate personnel to facilitate this activity. Ownership of identifying the risks correctly remains with line management.

   During risk identification care should be taken to identify 'inherent/gross' risk. Rather than concentrating on 'residual/ net' risk. If this is not done the organization will not know what its exposure will be should controls fail. Knowledge on the inherent risk also allows better consideration of whether there is over-control in place if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. Knowledge about both 'inherent' and 'net' risk is important because the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.

Risk Identification Methods

6. To identify risks one of the following methods are used:
   - Surveys.
   - Interviews.
   - Workshops.

7. Following is the illustrative list of questions which could be used for surveys/ interviews/ workshops:
   - From your perspective, what are your key business and/ or your area objectives?
   - What are some of the significant internal and external risks faced by the organization in the achievement of the business and area objectives?
   - From your perspective what is the likelihood of the risk occurring?

- From your perspective what is the consequence of the risk?
- What are some of the measurable performance targets and key performance indicators (KPIs) that can be linked to monitoring/mitigating the risks identified? (For example Budget to actual, ratings performance ranking).
- What is the frequency of measuring these KPIs?
- What other actions are taken to mitigate/ manage the risks identified?
- What is the frequency of these actions?
- Who is responsible for monitoring these risks?

Industry Risk Models

8. In addition to these generally used methodologies, industry-sector wise risk model can also be used. Generally these models are developed by professional organizations. Industry-sector model is helpful in identifying dynamic risks to which an organization is exposed to.

Which Method to Use ?

9. What is the most effective method or whether a combination of these methods should be used? This depends on various factors including the organizational culture, time available to complete risk identification, etc. Normally this comes with experience to the risk practioner.

Typical Risk Areas

10. Identification of the risks associated with business activities and decision making may be strategic/ tactical, project/ operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

11. During identification of internal risks it would be important to consider aspects as organizational structure, locations, objectives of the organization, key business processes and functions, strategic partners, outsourced service providers, etc.

12. During identification of external risks the political, economic, social and regulatory aspects in which the organization is functioning needs to be considered. Since identifying external risks is a complex activity generally organizations utilize forecasts and current events/ scenarios. Because of its complexity organization can utilize specialized external sources in this area.

13. An illustrative listing of areas in an organization where risk arises is given below:

Governance	Finance	Operational	Preparedness	Integrity
Authority	Funding	Quality	Morale	Management fraud
Leadership	Financial instruments	Customer service	Workplace environment	Employee fraud
Performance	Financial reporting	Pricing	Confidentiality	Illegal acts
Corporate directionand strategy	Foreign exchange /currency	Obsolescence	Communication flow	Unauthorized use
Incentives	Cash flow	Sourcing	Communication infrastructure	
	Investment evaluation	Product development	Change acceptance	
	Treasury	Product failure	Change readiness	
	Payroll	Business interruption	Challenge	
	Debtor/creditor management	Contingency Planning	Ethics	

Compliance	Environment	Human Resources	Reputation	Technology
Health and safety	Seasonality	Competencies	Brand	Reliability
Environment	Globalization	Recruitment	Reputation	Management information systems
Copyright and trademarks	Competition	Retention	Intellectual property	Access /availability
Contractual liability	E-commerce	Performance measurement	Stakeholder perception	IT security
Taxation	Share price	Leadership development		
Data protection	Strategic uncertainty	Succession planning		

Risk Estimation (or Risk Measurement/ Risk Scoring)

14. Risk estimation can be defined as 'assessing the impact of the risk on the organization.' During risk estimation the following should be kept in mind:
    - Difference between, inherent and residual risk needs to be established.
    - Ensure that there is a clear process methodology on risk estimation so that both likelihood and impact are considered for each risk.
    - Record the estimation of risk in a way which facilitates monitoring and the identification of risk priorities.

15. As discussed earlier all organizations are exposed to various categories and nature of risks, and quantitative methodology may not be sufficient and relevant to complete risk estimation. Hence qualitative characteristics and judgment, knowledge of the management on the organization needs to be utilized (example in the case of reputation risk - a subjective view is all that is possible). Hence risk evaluation is more of an art, than science.

16. Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence. The use of a well designed structure is necessary to ensure comprehensive risk identification, estimation and evaluation process. Different organizations will find their own measures of consequence and probability that will suit their needs best. For example many organizations find that assessing consequence and probability as high, medium or low is quite adequate for their needs and can be presented as a 3x3 matrix. Other organizations find that assessing consequence and probability using a 5x5 matrix gives them a better evaluation. If clear quantitative evaluation can be applied to the particular risk - "5x5" matrices are often used, with impact on a scale of "insignificant/ minor/ moderate/ major/ catastrophic" and likelihood on a scale of "rare/ unlikely/ possible/ likely/ almost certain".

Illustrations for measuring probability of occurrence and magnitude of impact of risk (5x5 criteria) are in Exhibit 1 and 2. Also refer to Para 2.4-2.8.

Risk Evaluation

17 When the risk estimation process for each risk has been completed, it is necessary to compare the estimated risks against risk criteria (i.e., risk appetite) which the organization has established. The risk criteria may include associated costs and benefits, legal requirements, socioeconomic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organization and whether each specific risk should be accepted or treated.

18. A common method of evaluation is to use a 'risk heat map'. The 'risk score' of a risk is the multiple of 'likelihood score' and 'significance score' which is adjusted by the qualitatitive assessment of the management. (Refer to Exhibit 3 for risk score). The risk heat map has likelihood of risks and impact of risks as the two axis and individual risks are plotted on it based on their risk score. Further a "traffic light" approach is used to show the risk, where green signifies do not require action, those which are amber should be monitored and managed down to green if possible, and those which are red require immediate action (refer to Exhibit 4 for risk heat map).

Usage of Risk Scores

19. From the management's perspective when it is reviewing the risk register for CEO/ CFO reporting purposes and giving a disclosure in the Annual accounts on the internal controls, it is not the inherent risk score but the residual risk score which is important; as management wants to assess whether the residual risk is regarded as tolerable, or how far the exposure is away from tolerability.

20. From the internal auditor's perspective it is the inherent risk score which is important as the internal auditor is to give an assurance on the design and adequacy of risk identification process as part of his overall assurance on the risk management process.

Appendix II

Score Card for Assessing Risk Maturity

A. Check list for Assessing Risk Maturity[8]

Risk maturity is the degree to which the organisation understands its risk and has implemented ERM.

a. Understanding on Objectives and their Associated Risks

1. The organisation's objectives are documented and understood.
2. Management has been trained to understand as to what risks are and their responsibilities for them.

b. Installation and Usage of Risk Management within the Organization

3. Process have been defined to determine risks and these have been followed.
4. A scoring system for assessing risks has been defined.
5. All risks have been assessed in accordance with the defined scoring system.
6. Response to the risks have been selected and implemented.

8 Based on An approach to implementing Risk Based Internal Auditing, IIA, UK and Ireland

7. The risk appetite has been defined using the scoring system.
8. Risks have been allocated to specific job titles in the risk register.
9. Management have set up monitoring controls on processes, responses and action plans.
10. Risks are regularly reviewed by the organization and the risk register updated.
11. Management report risks to Directors where responses have not managed risks the risks to a level acceptable to the Board.
12. All significantly new projects/ products are routinely assessed for risks.

c. Assessment on Managers Understanding and Usage of Risk Management

13. Responsibility for determination, assessment and management of risks is included in job description.
14. Managers provide assurance on the effectiveness of their risk management.
15. Managers are assessed on their risk management performance.

B. Suggested Scoring and its Interpretation

Score

0 - No

1 - Yes, Incomplete/ Possibly

2 - Yes.

Conclusion on Risk Maturity

0	-	7	:	Risk Naïve
8	-	14	:	Risk aware
15	-	20	:	Risk defined
21	-	25	:	Risk managed
26 and above			:	Risk enabled.

A. Risk Aware and Risk Naive

No risk register will be available in this type of organisation. As a consulting assignment, internal audit may be asked (in conjunction with management) to determine the work required to implement a risk framework which fulfils the requirements of the Board.

In such an organization, the focus of internal audit is necessarily on the controls. As same extent of risk assessment is in progress, some information on risks is available. The level of assurance on the controls would be higher if the internal auditor uses the key risks agreed with management to formulate the audit plan. The audit approach in this case would revolve around:

- Using the available information on risks during the planning stage for individual audits (discussed further in Chapter 4).
- Where management does not understand risks, conducting management training and risk facilitation workshops.

Despite a mention of the term "risks", the internal audit, as mentioned earlier, would provide assurance only on controls and not on the management of risks. Accordingly, the audit methodology is a modification of the traditional audit process and not RBIA. Also, care should be taken that as internal auditors are not primarily responsible for risk management, they should not determine risks without management involvement.

B. Risk Defined

In this type of organization, the understanding of risk management is patchy and the list of risks may not have been compiled into a complete risk register. As a consulting activity, internal audit in this case, would facilitate the compilation of a complete risk register from the list of risks already compiled by the managers. In areas where risk management is well defined, the internal auditor may use RBIA.

C. Risk Enabled and Risk Managed

This type of organisation represents a high level of understanding on the management of risk. A complete list of risks (risk register) is available for audit planning and the internal audit work would emphasize on whether risk management processes are working properly, responses to key risks and on the monitoring of controls.

of the organization are within acceptable levels as defined by the Board. Focus on risks and providing consulting and assurance services around a continuously updated *"risk register"* is probably the first step towards delivering to the management in accordance with their expectation and reducing the *"expectation gap"*.

Introduction to Risk-based Internal Audit

1.8. The objective of RBIA[1] is to provide independent assurance to the Board that:

- The risk management processes which management has put in place within the organisation (covering all risk management processes at corporate, divisional, business unit, business process level, etc.) are operating as intended.
- These risk management processes are of sound design.
- The responses which management has made to risks which they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the Board.
- And a sound framework of controls is in place to sufficiently mitigate those risks which management wishes to treat.

1.9. Hence the internal audit report is on the management of significant risks of the organization and the assurance is on these risks being managed within the acceptable limits as laid down by the Board of Directors.

To give this assurance the internal auditor would carry out:

- *a process audit on risk management processes at all levels of the organization, viz., corporate, divisional, business unit, business process level, etc.,* put in place by line management so as to assess the adequacy of their design and compliance.
- *a transactional audit on the significant risks* so as to assess whether the risk response puts the risk within acceptable limits.

By doing so, the RBIA methodology links the internal audit activity to an organisation's overall risk management framework. At the risk register level, the link between management of risks and its audit is done by adding the audit procedure, and other relevant audit information against each risk. This

1 Position Statement on RBIA issued by the Institute of Internal Auditors - UK and Ireland

set of documents is known as the risk and audit universe (RAU). *(Refer to Exhibit 6).*

Comparison with Traditional Internal Audit

1.10. RBIA is not different from internal audit. It represents internal auditing using a risk-based methodology. Under the traditional internal audit approach, the internal auditors are required to confirm that the controls are operating effectively. Internal auditors then make recommendations where the controls are not effective. Although traditional internal audit concentrates on riskier areas of the organisation, its approach is based on its own assessment of risk. RBIA bases itself on the underlying fact that the organisation's management is responsible for risk management across the organisation. It audits the risk management processes built by the management and if found reliable bases its audit efforts around management's assessment of risk. RBIA hence ensures that the audit resources are utilised towards assessing the management of most significant risks. RBIA approach has greater involvement of organisation's management as many risks being dealt with are very significant to the organisation. RBIA may involve audit of new areas in the organisation that internal auditors had not covered before. RBIA does not necessarily change the auditing techniques to be used. However, the audit tests and techniques under RBIA focus on ensuring the effectiveness of controls which treat risks. Neither are the tests specially designed to detect incorrect and fraudulent transactions, nor does it deploy resources on insignificant risks.

1.11. Internal auditors while following the RBIA methodology may also notice the following subtle differences during the assignment:

- Shift of focus from reviewing controls to reviewing risk.
- Extensive preparation required on understanding the macro economics of the industry, the positioning of the organization, its objectives, strategies and processes.
- Significant coverage of risks which are externally driven.
- Increased dependence on risk management documentation which links objectives, processes, risks, controls, and people.

- For organizations at a lower risk maturity level, performing both consulting and assurance activities.
- Redundancy of structured audit programs as individual risks are listed in the audit plan.
- Heightened management participation during all phases of the audit.
- Management pressure for an experienced multidisciplinary team whose members are first business managers and then internal auditors.

Before discussing the process of RBIA in detail, it is important to understand 'risks' and 'risk management'.