Internal Audit – in Risk Management Approach

RADU FLOREA,
RAMONA FLOREA
George Bacovia University, Bacău, ROMANIA
radu.florea@ugb.ro
ramona.florea@ugb.ro

Key words: *Internal audit, risk, ERM, COSO framework*
Abstract: This paper aims to present a modern approach of the internal audit function based on risk identification and assessment. The issue is composed in three parts, including a general presentation of internal audit profesion, COSO framework and the methodology of Risk identification and assessment.

1. An overview of internal audit profession

"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."[1]

The scope of internal auditing within an organization is broad and may involve topics such as the efficacy of operations, the reliability of financial reporting, deterring and investigating fraud, safeguarding assets, and compliance with laws and regulations.

Internal auditing frequently involves measuring compliance with the entity's policies and procedures. However, Internal auditors are not responsible for the execution of company activities; they advise management and the Board of Directors (or similar oversight body) regarding how to better execute their responsibilities.

The Internal Auditing profession evolved steadily with the progress of management science after World War II. It is conceptually similar in many ways to financial auditing by public accounting firms, quality assurance and banking compliance activities. Much of the theory underlying internal auditing is derived from management consulting and public accounting professions. With the implementation in the United States of the Sarbanes-Oxley Act of 2002, the profession's growth accelerated, as many internal auditors possess the skills required to help companies meet the requirements of the law.

The objectives of early internal auditors were primarily built around the protection of assets and detection of fraud. Consequently, the auditors concentrated most of their attention on examinations of financial records and on the verification of assets that were most easily misappropriated. A popular idea among management people a generation ago was that the main purpose of an auditing program was to serve as a psychological deterrent against wrongdoing by other employees.

The internal auditing function has undergone significant changes in the last century. The main objective of the Internal Audit function has moved from that of fraud detection to assisting management in making decisions beginning with a risk assessment. The Internal Audit staff of today is considered a good training ground for management-level personnel, but many organizations have outsourced the entire IA function.

Also in the 1990s, one trend caused a change in the way the Internal Audit function was carried out. Outsourcing became a popular way for organizations to employ the Internal Audit function. The role of the Internal Audit function was served by public accounting and other providers. The IIA Standards and Statement have evolved further and now have the cornerstone of risk assessment.

[1] http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/

In present days, knowing about and understanding both internal and external risks that can potentially impact the organization, and ensuring that these risks are managed to an optimal level, should be top priorities for board and audit committee members. This is enterprise risk management (or ERM).

ERM helps ensure effective reporting and compliance with laws and regulations and helps prevent losses — whether in the form of revenues or reputation. An ERM approach to risk is applicable to any organization, regardless of its industry or sector. Inherent in the ongoing ERM process are a variety of activities that help an organization achieve its performance and profitability targets. These include aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities, and improving deployment of capital.

2. COSO Framework and Internal Audit approach

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) states that ERM is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO comprises five major professional associations: The Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

COSO's Enterprise Risk Management — Integrated Framework defines essential components, suggests a common language, and provides clear direction and guidance for ERM. Enterprise risk management requires an entity to take a "portfolio" view of risk, which examines the entire organization, from the enterprise level to a division or subsidiary, to the level of a single business unit's processes.

Within the context of an entity's mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise in four categories:

- Strategic – high-level goals, aligned with and supporting its mission.
- Operations – effective and efficient use of its resources.
- Reporting – reliability of reporting.
- Compliance – compliance with applicable laws and regulations.

This categorization of entity objectives allows a focus on separate aspects of ERM while taking a holistic approach to risk, and enabling management to consider how individual risks interrelate. The distinct but overlapping categories, as well as safeguarding of resources, address different entity needs and may be the direct respon sibility of different executives.

ERM must be integrated with management processes. It examines eight interrelated components:

1. Internal Environment – management sets a risk philosophy and establishes the entity's risk culture and risk appetite.
2. Objective Setting – management considers its risk appetite in the setting of objectives.
3. Event Identification – management identifies the events, both internal and external, that present risk or opportunity to the organization. Opportunities are channeled back to strategy and objective-setting processes.
4. Risk Assessment – the likelihood and impact of risks are assessed to clarify the extent to which they might impact objectives. This employs a combination of qualitative and quantitative methodologies and forms a basis for the management of those risks.
5. Risk Response – management makes the decision as to whether the risk should be avoided, accepted, reduced, or shared; and then develops a set of ac tions to align the risks with the organization's risk tolerance.
6. Control Activities – policies are established to ensure manage ment's risk responses are carried out effectively.
7. Information and Communication – thorough and timely communica tion takes place to ensure roles and responsibilities can be performed effectively in the process of identifying, assessing, and responding to risk.
8. Monitoring – ongoing ERM monitoring occurs, and modifications are made as warranted.
   According to this the COSO – ERM Framework is show in Fig. 1.

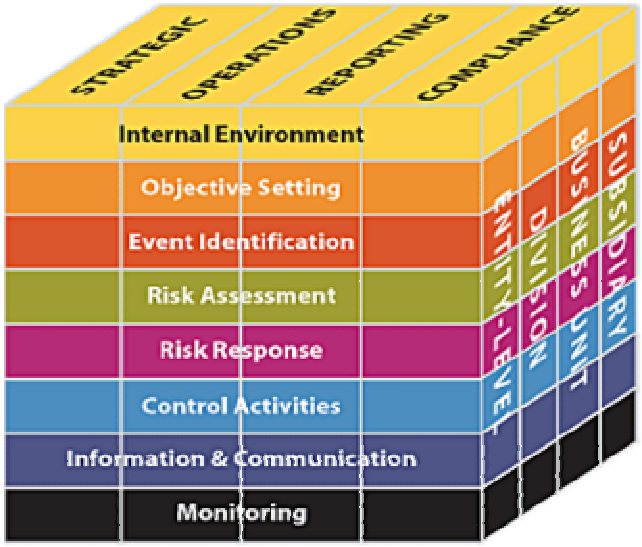


Fig. 1 – COSO Famework

All managers have to make decisions in the face of uncertainty. Risk is the possibility that they will experience adverse consequences from these decisions, or not successfully exploit the opportunities that become available. The objective of risk management is to enable managers to take risks knowingly, reduce risks where appropriate and strive to prepare for a future that cannot be predicted with absolute certainty.

Risk management is not the responsibility of the internal audit function. Management may require internal audit to perform the function but this means the involvement of internal audit in the day-to-day running of the business which can impair auditor objectivity. Many large organisations have separate risk management functions. Internal audit's job may be to assist that function or the board by:

- providing objective assurance on the adequacy and effectiveness of the risk management and internal control framework;
- helping improve the processes by which risks are identified and managed;
- helping strengthen and improve the risk management and internal control framework.

Internal audit can provide advice on the design, implementation and operation of control systems, identify opportunities to make control cost savings, and promote a risk and control culture within the organisation.

Internal auditors can also act as facilitators, guiding managers and staff through a self- assessment process, perhaps by leading workshops. Internal audit can also become a centre of expertise for managing risk by providing enterprise-wide risk management services.

In order to do all of this, internal audit needs to be aware of how risk management works.

Any system of risk management and internal control needs to be aligned with business objectives. Business objectives and risks relating to those objectives can be classified in many ways. One classification is as follows:

- effectiveness and efficiency of operations (including profitability customer service, and corporate responsibility, for example);
- reliability of internal and external reporting (i.e. internal financial control);
- compliance with internal and external regulations.

Another classification might be as follows:

- business risks (relating to the economy, technology and competition, for example);
- financial risks (relating to liquidity, interest rates, exchange rates and the misuse of financial resources, for example);
- compliance risks (such as a breach of stock exchange regulations, non-compliance with accounting standards or company law, and non-compliance with tax or environmental regulations, for example);
- operational risks (such as loss of assets, poor service levels, employee-related issues, or a shortage of raw materials, for example).

3. The methodology of risk identification and assessment

Risk management is a dimension of good management that requires the following steps:

- establish a business framework;
- identify all significant risks;
- measure risks;

- deal with the most important risks;
- monitor arrangements.

3.1. Establish a business framework

A clear business framework should be developed for risk management. This should be documented within a formal risk management policy and should include: the corporate attitude to risk and its risk appetite; the types and levels of risk that are considered acceptable; responsibilities for risk management; risk should be considered during all management initiatives, but specific risk management aspects should be assigned to named managers; an outline of the formal risk management procedures, review and reporting timetables; procedures to ensure a suitable level of risk awareness and communication across the organisation.

The setting of clear, documented corporate and departmental objectives is a precondition for risk management. Responsibility for risk management rests ultimately with the board (or equivalent) who should retain responsibility for the major risks the organisation faces. However, all levels of managers and staff should be responsible and actually feel they have responsibility for the management of risk in their particular area.

3.2. Identify all significant risks

Effective managers should be aware of the risks in their area of responsibility. However, each organisation will benefit from ensuring that the identification and assessment of risks is conducted in a structured way at each level within its management hierarchy. This should include a top down approach at corporate level; a bottom up approach at departmental or section level; and an analysis of the links between these two approaches.

The senior management team and departmental managers should be responsible for conducting a detailed identification of the risks the organisation faces in achieving its corporate objectives. Meetings should be held with groups of managers at each level within the organisation to: brainstorm risks facing each activity undertaken; identify existing controls to mitigate risks and further action that is necessary; identify named managers responsible for each risk and associated control action; agree the monitoring action to be undertaken.

In some organisations, risk management has developed from the insurance function. However, risk management should be concerned with more than just the insurable risks. It includes all the uncertainties and opportunities that an organisation faces. These risks may be analysed as follows:

- political/policy;
- corporate issues;
- personnel issues;
- financial;
- commercial;
- legal/regularity;
- health and safety;
- operational;
- reputational.

In order to provide a structure for risk analysis, and to help allocate responsibility for managing different types of risk, risks need to be categorised appropriately. One method of risk classification is to reflect broad business functions, grouping risks relating to production, information technology, finance, and so on. However, directors also have to ensure that there is effective management of both the few risks that are fundamental to the organisation's continued existence and prosperity, and the many risks that impact on day-to-day activities, and have a shorter time frame compared with longer-term strategic risks. These two types of risk can be categorised as **strategic** and **operational** respectively. Having categorised risks, management can then analyse the probability that the risks will materialise and the hazard (impact or consequences) if they do materialise.

Strategic risks are those that arise from the fundamental decisions that directors take concerning an organisation's objectives. Essentially, strategic risks are the risks of failing to achieve these business objectives. A useful subdivision of strategic risks is:

Business risks – risks that derive from the decisions that the board takes about the products or services that the organisation supplies. They include risks associated with developing and marketing those products or services, economic risks affecting product sales and costs, and risks arising from changes in the technological environment which impact on sales and production.

Non-business risks – risks that do not derive from the products or services supplied. For example, risks associated with the long-term sources of finance used.

Strategic risk levels link in with how the whole organisation is positioned in relation to its environment and are not affected solely by what the directors decide. Competitor actions will affect risk levels in product markets, and technological developments may mean that production processes, or products, quickly become aut-of-date.

Operational risks - Although boards need to incorporate an awareness of strategic risks into their decision making, there is a danger that they focus excessively on high-level strategy and neglect what is happening 'on the ground' in the organisation. If production is being disrupted by machine failure, key staff are leaving because they are dissatisfied, and sales are being lost because of poor product quality, then the business may end up in serious trouble before all the exciting new plans can be implemented. All of these are operational risks – risks connected with the internal resources, systems, processes, and employees of the organisation.

Some operational risks can have serious impacts if they are not avoided. Other operational risks may not have serious financial (or other) impacts if they only materialise once or twice. However, if they are not dealt with effectively, over time – if they materialise frequently – they can result in quite substantial losses.

When identifying risks many managers will identify the symptoms of risk. However, to enable risks to be effectively managed the underlying reason for the risk exposure (its cause) will have to be identified.

3.3. Measure risks

There are two aspects or dimensions to measuring risk:

- the impact of the risk - what is the potential damage that the organisation faces?
- the likelihood of the risk - how likely is it that the damage will occur?

One approach to measuring risks is by assigning values and probabilities to each risk. The usual method of scoring risks is to assign a level (e.g. high, medium, low), or score (e.g. 1 to 5) to the consequence and likelihood of the risk. Where levels are assigned a numerical value, consequence and likelihood scores may be combined (for example, by multiplication, or by ranking on a grid) to provide an overall score. So for example, the score of the highest risk would be 25 on this basis, when using a 1 to 5 scoring range.

Risks are often placed on a grid as follows:

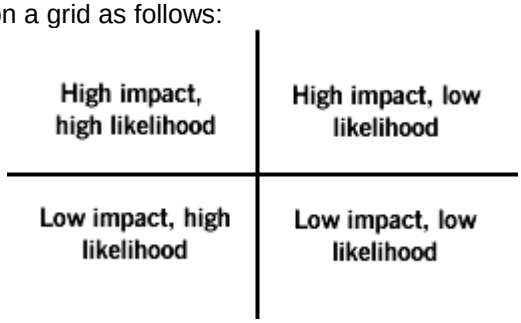
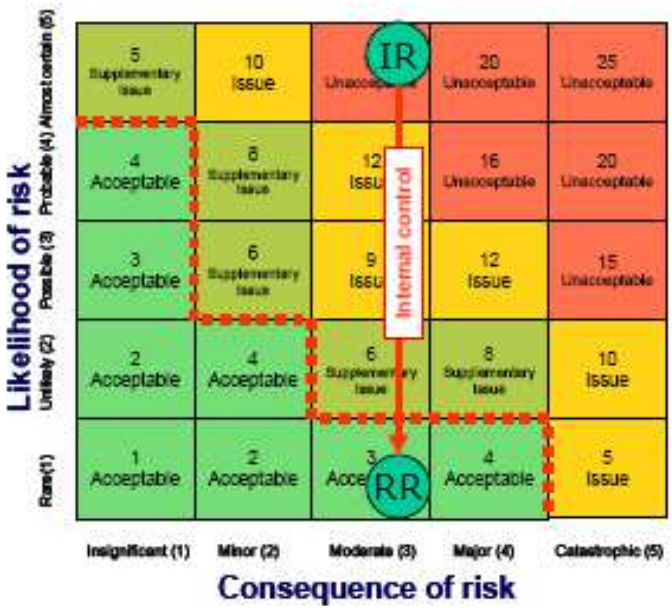


Fig. 2 – Likelihood – Impact matrix

The approach adopted should be kept as simple as possible. At one extreme risks could just be assigned to one of the four quadrants in a risk evaluation matrix such as the one included opposite. As a compromise the impact and likelihood of a risk could be identified as being high, medium or low.

A number of organisations have found that control self-assessment type workshops are a useful means of identifying and assessing the significance of the risks that the organisation faces. In this case a facilitator can help a group of managers to brainstorm the full range of risks that exist. They will then collectively determine the significance of each of the individual risks.

The assessment and classification of risk will be different for each company and internal audit can help management by commenting on the criteria used for classification, for example and on how the criteria have been applied.



Unacceptable: Immediate action required to manage the risk
Issue: Action required to manage the risk
Supplementary issue: Action is advisable if resources are available
Acceptable: No action required
■ ■ ■ ■ ■ ■ Risk appetite
IR = Inherent Risk, RR = Residual Risk

Fig. 3 Grid showing the significance of risks

3.4. Deal with the most important risks

The process of identifying and measuring risks may be referred to as risk profiling. Once the risks have been profiled the most important should be reviewed to ensure that they are being effectively managed. There are four main ways of dealing with risks:

- accept;
- reduce;
- avoid;
- transfer.

Risks may be **accepted** if they have a low impact or are not likely to occur. Risks with a high impact but low likelihood may be accepted, but plans should be developed to ensure the continuation of the smooth running of the organisation if they crystallise.

Risks may be **reduced** by improving internal controls by, for example implementing internal audit recommendations. Risks need not, and often cannot, be eliminated, but they should be reduced to a level that is acceptable to the organisation.

If the risk is too great for the organisation and it is not practical to reduce the risk then the risk should be **avoided**.

Insurance is the usual way of **transferring** risks especially high impact risks that cannot be accepted. As an alternative the risk may be transferred by contracting out certain functions or through joint ventures.

3.5. Monitor arrangements

Once the key risks of the organisation, department or section have been identified, assessed and appropriate action determined, this process should be monitored and kept under review. A full review of the risks that the organisation faces should be undertaken at least once every three years. In addition, each year the risk management process at each level within the organisation should be formally reviewed. The risks that have crystallised and any changes to the impact or likelihood of each significant risk should also be considered.

One way to achieve this is to combine this process with existing business planning routines such as revising the strategic plan or developing annual budgets. This could be achieved by requiring managers to complete and report risk matrices or maps for their area of responsibilit. An example of a possible format for such a risk matrix is shown.

Where necessary further action should be agreed to deal with unacceptable outstanding risks. Departments should report to senior management and senior management should report to the Board on the results of this risk review process.

Conclusions

A proper system of internal control in practice requires a proper system of risk management and organisational control. This article focuses on the risk management element of internal control and how internal audit can assist in this area. Risk management is now an important feature of management in both the public and private sectors.

The higher profile of risk management in recent years has led some internal auditors to consider developing a risk-based approach to internal audit. However, risks do not exist in isolation. They are the results of the objectives of the organisation or system not being achieved. Risks should be considered as an integral part of the systems approach to internal audit. This should allow the adequacy and reliability of the existing controls to be considered within the context of the overall system that is being audited.

Endnotes

David Griffiths, 2005, *Internal Auditing – A risk based approach,* http://www.internalaudit.biz/IIA, 2007, *A holistic view of risk,* http://www.theiia.org/

PricewaterhouseCoopers, 2007, *State of the internal audit profession study: Pressures build for continual focus on risk,* http://www.pwc.com/us/en/internal-audit/publications

http://www.aair.ro/
http://www.coso.org
http://www.ifac.org
http://www.kpmg.com/global
http://www.pwc.com
http://www.theiia.org/