

Internal Audit and Risk Management. ISO 31000 and ERM Approaches

Radu FLOREA, Ramona FLOREA
George Bacovia University, Bacau, ROMANIA
radu.florea@ugb.ro
ramona.florea@ugb.ro

Abstract: Risk management is an important part of the strategic management of any organization and it is the modality to identify positive and negative aspects of risks, representing the possibility of an event occurring that will have an impact on the achievement of objectives. In this context, an important role belongs to the internal audit to help an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. For this purpose, a lot of risk management standards have been issued, including the international standard ISO 31000 'Risk management – Principles and guidelines', which establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture. Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives. This paper wont to present an approach of Risk Management from ISO 31000 and ERM point of views.

Keywords: Internal Audit, Risk Management, ISO 31000, ERM (Enterprise-wide risk management)

Introduction

The IIA's (Institute of Internal Auditors) International Standards define a risk as “the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood”.

In actual economical context, for most organisations, risk management is the modality to identify positive and negative aspects of risks. In general theory of risk management, managing things that could have an adverse impact (downside risk) could also bring for companies potential benefits (upside risk). This approach could be applied holistically, but also could be used on specific activities of a company, from the strategic to the operational.

In this condition, risk management became an important part of the strategic management of any organisation. A successful risk management initiative in any organization should according to the level of risk in this organisation, and should be aligned with other corporate activities. Also he must be comprehensive and dynamic, being responsive to changing circumstances.

Each organization need to understand that when they want to achieve objectives (the reward) they takes some specific risks. In fact, organisations need to understand the overall level of risk embedded within their processes and activities. It is important for organisations to recognise and prioritise significant risks and identify the weakest critical controls. In this case an important role belongs to internal audit which 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.

All the risks that could affect an organization can have multiple consequences such as: perturbation of economic performance, effect on professional reputation, environmental and social problems, etc. In
conclusion, managing risk could help organizations to perform well in an environment full of uncertainty.

In fact, the global financial crisis demonstrated the importance of an adequate risk management. Since that time, a lot of risk management standards have been issued, including the international standard ISO 31000 “Risk management – Principles and guidelines”.

1. ISO 31000 Approaches of Risk Management
There are many opinions regarding what risk management involves, how it should be implemented and what it can achieve. International Organisation for Standardisation (ISO) standard 31000 was published in 2009 and seeks to answer these questions.

ISO is a worldwide federation of national standards bodies (ISO member bodies). ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization. International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. In this case, ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. ISO 31000 describes this systematic and logical process in detail.

The focus of risk management is the assessment of significant risks and the implementation of suitable risk responses. The objective is to achieve maximum sustainable value from all the activities of the organization. Risk management enhances the understanding of the potential upside and downside of the factors that can affect an organization. It increases the probability of success and reduces both the probability of failure and the level of uncertainty associated with achieving the objectives of the organization.

While all organizations manage risk to some degree, the ISO 31000 establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization’s overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of “establishing the context” as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.
The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in ISO 31000 are shown in Figure no. 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- be aware of the need to identify and treat risk throughout the organization;
- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;
- improve mandatory and voluntary reporting;
- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;
- minimize losses;
- improve organizational learning; and
- improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;
b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
c) those who need to evaluate an organization's effectiveness in managing risk; and
developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of ISO 31000. In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

2. Internal Auditing’s Role In Risk Management

The first question to consider is, “What are internal auditors being asked to do?” It is important to understand the direction that is being provided by the board of directors, typically through the audit committee (to whom most internal audit activities report functionally) and management (to whom most internal audit activities report administratively).

In August 2009, a Global Audit Information Network (GAIN) Flash Survey with 321 respondents identified the following when it asked about the direction provided by the audit committee:

<table>
<thead>
<tr>
<th>Has the audit committee asked internal auditing…</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>to provide an opinion on any individual programs or areas related to risk management?</td>
<td>41%</td>
<td>59%</td>
</tr>
<tr>
<td>to provide an opinion on the organization’s overall risk management processes?</td>
<td>23%</td>
<td>77%</td>
</tr>
<tr>
<td>to perform specific audits of any components of risk management?</td>
<td>28%</td>
<td>72%</td>
</tr>
<tr>
<td>for recommendations or advice on enhancing the organization’s risk management processes?</td>
<td>45%</td>
<td>55%</td>
</tr>
</tbody>
</table>

While it is difficult to conclude why these percentages are not higher, one answer may be found in another question from that survey. Respondents were asked “How much do you agree or disagree that there is an emerging need for the audit committee to have better insight into the organization’s risk management processes?” The answers to this question were:

| Strongly Agree | 37% |
| Agree | 38% |
| Neutral | 5% |
| Disagree | 1% |
| Strongly Disagree | 19% |

Three quarters of the respondents believed that there is an emerging need for audit committees to gain more insight into risk management processes. It is reasonable to presume that a lack of general awareness and understanding about risk management results in a lower level of appreciation of how internal audit activities can provide meaningful insights and assurance surrounding risk management activities. It is also possible that audit committees do not perceive that internal auditors possess the right skills and experience to assess risk management activities.

Despite the modest level of top-down direction received from the audit committee and management, internal audit activities have made strides in playing a role in risk management and will continue to do so. The 2010 IIA Global Internal Audit Survey (a component of the Common Body of Knowledge [CBOK] studies) indicated that 57 percent of internal audit activities around the world perform audits
of enterprise risk management processes. Furthermore, 20 percent of respondents indicated that they believed performing such audits would become more prominent over the next five years.

An IIA Position Paper titled *The Role of Internal Auditing in Enterprise-wide Risk Management* provides an illustration that presents a range of risk management activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should not undertake.

Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

In this case, Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management. The two most important ways that internal auditing provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively. The activities included in ERM are often:

- Articulating and communicating the objectives of the organization;
- Determining the risk appetite of the organization;
- Establishing an appropriate internal environment, including a risk management framework;
- Identifying potential threats to the achievement of the objectives;
- Assessing the risk (i.e. the impact and likelihood of the threat occurring);
- Selecting and implementing responses to the risks;
- Undertaking control and other response activities;
- Communicating information on risks in a consistent manner at all levels in the organization;
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing assurance on the effectiveness with which risks are managed.

In Figure no. 2, the five areas on the left of the “fan” represent core internal audit roles for risk management. These activities are all assurance activities. The position paper states that “They form part of the wider objective of giving assurance on risk management. An internal audit activity
complying with the *International Standards for the Professional Practice of Internal Auditing* can and should perform at least some of these activities.” It appears that the majority of internal audit activities are falling short of this strongly recommended guidance.

Internal auditing may provide consulting services that improve an organization’s governance, risk management, and control processes. The extent of internal auditor’s consulting in ERM will depend on the other resources, internal and external, available to the board and on the risk maturity of the organization and it is likely to vary over time.

Internal auditor’s expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that the internal audit activity is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction. As the organization’s risk maturity increases and risk management becomes more embedded in the operations of the business, internal auditing’s role in championing ERM may reduce. Similarly, if an organization employs the services of a risk management specialist or function, internal auditing is more likely to give value by concentrating on its assurance role, than by undertaking the more consulting activities. However, if internal auditing has not yet adopted the risk-based approach represented by the assurance activities on the left of Figure no. 2, it is unlikely to be equipped to undertake the consulting activities in the center.

The seven areas in the middle of the “fan” represent legitimate internal audit roles with appropriate safeguards. While the position paper lists several safeguards that can be taken, generally they focus on not taking on decision-making or other management roles, such as those depicted in the right part of the fan. These legitimate internal audit roles are generally considered consulting roles that can greatly enhance the value provided by internal auditing in risk management. While few of these were specifically considered in the survey, the results indicate that most internal audit activities are not performing these valuable roles.

The six areas on the right are roles that internal auditing should not undertake because they are management responsibilities that would clearly impair the internal audit activity’s objectivity. For those that were included in the survey, it is encouraging that few internal audit activities appear to be taking on these types of roles.

**Conclusions**

Risk management is a fundamental element of corporate governance. Management is responsible for establishing and operating the risk management framework on behalf of the board. Enterprise-wide risk management brings many benefits as a result of its structured, consistent and coordinated approach. Internal auditor’s core role in relation to ERM should be to provide assurance to management and to the board on the effectiveness of risk management. When internal auditing extends its activities beyond this core role, it should apply certain safeguards, including treating the engagements as consulting services and, therefore, applying all relevant Standards. In this way, internal auditing will protect its independence and the objectivity of its assurance services. Within these constraints, ERM can help raise the profile and increase the effectiveness of internal auditing.

**Supplementary recommended readings**


The role of Internal Auditing in Enterprise wide Risk Management (january 2009), [https://na.theiia.org/standardsguidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf](https://na.theiia.org/standardsguidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf)

www.iia.org

www.theirm.org

77