RISK MANAGEMENT: AN INTEGRATED APPROACH TO RISK MANAGEMENT AND ASSESSMENT

Szabo Alina
Member of the Institute of Internal Auditors (IIA)

Purpose:
The objective of this paper is to offer an overview over risk management cycle by focusing on prioritization and treatment, in order to ensure an integrated approach to risk management and assessment, and establish the 'top 8-12' risks report within the organization. The interface with Internal Audit is ensured by the implementation of the scoring method to prioritize risks collected from previous generated risk report.
Methodology/approach:
Using evidence from other research in the area and the professional expertise, this article outlines an integrated approach to risk assessment and risk management reporting processes, by separating the risk in two main categories: strategic and operational risks. The focus is on risk prioritization and scoring; the final output will comprise a mix of strategic and operational ('top 8-12') risks, which should be used to establish the annual Internal Audit plan.
Originality/value:
By using an integrated approach to risk assessment and risk management will eliminate the need for a separate Internal Audit risk assessment over prevailing risks. It will reduce the level of risk assessment overlap by different functions (Tax, Treasury, Information System) over the same risk categories as a single methodology, is used and will align timings of risk assessment exercises.
The risk prioritization by usage of risk and control scoring criteria highlights the combination between financial and non-financial impact criteria allowing risks that do not naturally lend themselves to a financial amount to be also assessed consistently.
It is emphasized the usage of score method to prioritize the risks included in the annual audit plan in order to increase accuracy and timelines.
Keywords: risk management, risk assessment, audit universe.
JEL cods: G320

1. Introduction

Risk management is a range of activities undertaken to control the strategic and operational risks within the organization. It can be defined as a business process whose purpose is to ensure that the organization is protected against risks and their effects.
In The Project Management Body of Knowledge Guide, (Duncan, W., R., 1996), risk management is defined as a systematic process of identification, analysis and response to the project risks, process comprising the risk identification, risk quantification, risk response plan, risk response control sub processes. By a closely look the reader can observe that, depending on the author of the methodology, the name or the order of these sub-processes is different. Thus, risk identification and risk quantification are sometimes taken together and are called risk assessment or risk analysis; the risk response plan is sometimes met under the name of risk mitigation plan; the risk response plan and the risk control plan are sometimes taken together under the name of risk management plan. (Valentin P. Mazareanu, Risk Management and Analysis: Risk Assessment (Qualitative and quantitative), Analele UAIC Iasi, 2007)
Going further, we can affirm that, without risk, there is no reward or progress. Unless risk is managed effectively, organizations cannot maximize opportunities and minimize threats. Risk is all about uncertainty, or more importantly, the effect of uncertainty on the achievement of objectives. By performing the risk management process steps, the emphasis is shifted from

something happening – the event –to the effect on objectives. Every organization has objectives to achieve, and in order to achieve them, any uncertainty that could interfere with their realization must be effectively managed. (Kevin W. Knight AM, Main Focus Magazine, ISO FOCUS, 2009)
As stated in the well-stocked toolbox for risk management featuring (ISO 31000:2009 –Risk Management –Principles and guidelines; ISO/IEC 31010: 2009 – Risk management –Risk assessment techniques): "Risk needs to become an integral part of how things are managed*; it should* not be an add-on, or a separate activity divorced from the mainstream management of the business." This refers to the mandate and commitment of the organization's board and top management to the implementation, review and continual improvement of how risk is managed. The end goal: to ensure risk is fully focused on the achievement of objectives by using a common language and process throughout the organization.
As related to risk management reporting responsibility, the organization has to nominate a Risk Coordinator to facilitate the internal risk assessment and reporting process. Unless there is any top management person appointed to be the company's Risk Coordinator, it is anticipated that this will be the local Head of Internal Audit; although it is possible for the coordinator to come from any discipline. If this happens, the organization should ensure local Internal Audit is involved in the risk assessment. This will help ensure they have sufficient understanding of the risk assessment process and outputs to enable them to develop a risk-based internal audit plan.

2. Inside Risk Management: overview of risk management reporting process

We will present an overview of the approach to risk management starting from the main idea that: "Risk management is a range of activities undertaken to control the strategic and operational risks within the organization." Underpinning the approach is an initial separation of the strategic and operational risk assessment processes, recognizing that they serve different purposes. The key definitions of the two main risks are below:

-Strategic risks are uncertain future events that could negatively impact the achievement of the vision and strategic objectives.

-Operational risks are risks that could negatively impact the performance or efficiency of the day-to-day operations.

The Strategic risk report should be used to summarize the key strategic risks faced by the organization that could negatively impact on the achievement of their vision and strategic objectives. The strategic risks detailed in the risk report represent the inherent strategic risks before taking account of any risk responses.
Once the key strategic risks have been identified, the risk responses which are currently relied on to reduce the inherent level of a risk to a more acceptable level need to be detailed. Consideration should be given to operational risks that are sufficiently significant/ material that they may have strategic consequences. The strategic risk report will have a dual purpose of supporting the strategy and planning process and as an integral part of the risk management process.
The first step in the operational risk assessment is to identify potential inherent risks using the Risk Universe tool. This Risk Universe contains risk categories grouped under value chain and support headings. It is not intended to be a comprehensive list of all operational risks but it should assist in ensuring all the relevant risk issues for the business are incorporated within the assessment process. Using the categories contained in the Risk Universe, it should be involved the relevant management staff in the risk assessment process to make the outputs accurate and reliable by considering different risk assessments that need to be prepared. There is no set number of separate operational risk assessments prescribed. Examples of sub-categories of operational risks within risk universe are:

Value chain:

-*Sales and Marketing:* customer understanding, customer relationships, exclusivity arrangement, pricing and profitability, promotion and brand management, innovation;

-*Procurement*: quality, scheduling, costs, commodity exposure management;
-*Manufacturing*: efficiency, quality, capacity, product recall, product security;
-*Health and Safety*: incident management, regulatory reporting, preventive programs;
-*Physical assets*: safeguarding and security, business interruption, natural perils;
-*Warehousing and distribution*: logistic, obsolesce, loss/damage, cost, distribution channel;
-*Invoice and service customer*: customer support, credit control, billing completeness& accuracy, product/service failure;

Management and support:

-*Improvement and change:* cost control, realization of planned benefits;
-*Human resources:* incentives & remuneration, recruitment & retention, unethical behavior;
-*Financial Management:* reporting, fraud, budgeting & forecasting, insurance, treasury;
-*Legal and compliance:* contracting, litigation management, regulatory reporting, intellectual property;
-*Taxation:* tax legislation, customs & excises, documentation, planning;
-*Information resources and technology:* strategy, integrity, security, obsolescence, availability;
-*Sustainable development and environment:* energy efficiency, supply chain, resource availability;
-*Corporate affairs:* communication, reputation management, community affairs.

Once the key operational risks have been identified, the controls which are currently relied on to reduce the inherent level of a risk to a more acceptable level need to be detailed.

The next steps in risk assessment process should be their prioritization as "high", "medium" or "low", according to the criteria outlined below. Each risk should be prioritized on a "current" basis (assuming the application of existing risk treatment). Prioritizing risks will involve judgment, but the criteria below, evaluated in the context of the local business are designated to help ensure that the prioritization process is more consistent. In this order each risk will be scored according to likelihood and impact, using consistent and defined assessment criteria:

Likelihood – taking into account the risk responses in place over the risk, assess the probability that the risk event will occur in the organization. If it is highly likely (>50%) that the risk event will occur (for example, it can be anticipated to happen within 5 years or is already occurring in the company, or a similar organization has experienced such an event), then the likelihood is "high". If it is reasonably likely (25% - 50%) that the risk event will occur (for example the event can be envisaged within 5 years but may not have occurred yet in this area or in the company), then the probability is "medium". If it is unlikely (<25%) that the risk event will occur (for example the event is considered very difficult to realize within 5 years and only under exceptional circumstances in the company, or has not occurred in a similar organization) then the probability is "low".

Impact – should the risk event occur; assess the impact that this would have on the organization. It should be consider not only financial but also nonfinancial impact, because the nonfinancial impact criteria allow risks that do not naturally lend themselves to a financial amount to be also assessed consistently. The highest non-financial impact rating for a particular risk should be used in the risk report. If there would be a highly damaging impact to the financial results or reputation of the organization, then the impact is "high". For example, the event would result in >10% impact on budget/ EBITA, or serious production disruption, or a major safety/ environmental incident or breach of regulatory requirements, or sustained media coverage.

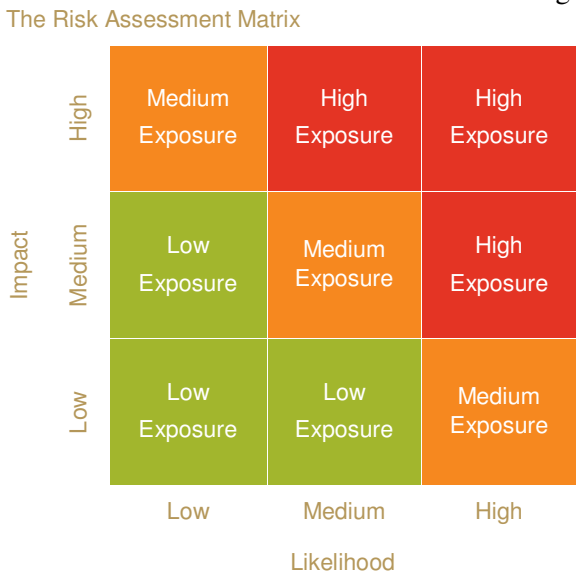
If the impact to financial results or reputation would be significant, but not highly damaging, then the impact is "medium". For example the event would result in 2-10% impact on budget/ EBITA, or some production disruption, or a significant but limited safety/ environmental incident

or breach of regulatory requirements, or limited media coverage. If the impact of financial results or reputation would be not particularly significant then the impact is "low". For example the event would result in <2% impact on budget/ EBITA and minimal production, regulatory or media impacts. The table below contains the classification of financial and non-financial impact as described: (Table 1)

Table 1: Classification of Impact

Financial	Production	Compliance	Reputation
>10% of budget/EBITDA	Serious production disruption	Major safety/environmental incident Major breach of regulatory requirements	Sustained media coverage International media coverage
2- 10% of budget/EBITDA	Some production disruption	Significant but limited safety/environmental incident Significant but limited breach of regulatory requirements	Limited media coverage National media coverage
<2% of budget/EBITDA	Minimal production disruption	Minimal safety/environmental incident Minimal breach of regulatory requirements	Minimal media coverage

Overall priority – Once the likelihood and impact of the current strategic or operational risk has been assessed then use the matrix below to assign an overall priority to the risk. (Fig.1)



There may be some risks within the business where actions are still under development to control the risk. Where this is the case, it should be described what further actions the organization is taking to address these areas, together with the expected timescale to complete the actions and the person responsible. The overall planned risk, if these further actions were implemented also needs to be identified and included in the risk report.

After the completion of previous steps, the information captured in strategic and operational risk reports should be finalized and checked for accuracy by the Risk Coordinator. Even if the Risk

Coordinator is facilitating the 'top 8-12' risk determination process, the decisions should involve either the senior management or the preferred option of Risk Governance Committee.
The strategic risk report and the operational risk reports should then be collated and the 'top 8-12' current risks for the organization determined. These will comprise a mix of strategic and operational risks and will be a judgmental issue given the different types of risks being considered.
An effectiveness review over the risk assessment and risk management reporting process should be performed at periodic intervals to satisfy corporate governance requirements and identify any further opportunities to increase efficiency and effectiveness.

Interface with Internal Audit

The detailed operational risk assessment process (and to a lesser degree the strategic risk assessment) will be used by Internal Audit for the purpose of completing their annual plan. This risk report will identify prevailing higher risk areas that may require further review or assurance by Internal Audit in the upcoming year. These risks are likely to include strategic and operational risks. The need for Internal Audit to produce a separate risk assessment to determine these prevailing higher risk areas will therefore be eliminated.
In addition to the prevailing risks above, Internal Audit is required to identify and review additional areas, based on inherent process risk or compliance requirements, where risks may be static. Some additional flexibility should continue to be retained in the Internal Audit plan, to respond to any further ad-hoc requests for Internal Audit reviews from senior management.
Based on the risk report previous described, the Internal Audit will score the risks by considering the following: time since fraud was identified in this area; calculated gross risks and net risks based on the risk assessment matrix (see up) and transforming them in cumulative gross and net risks; time since last audit; significance of past audit findings in this area; significance of trial balances (use balance sheet accounts and income statement accounts). The scores might vary between 1 and 30, depending on their identified relevance; the total range obtained by each risk will be the basis of the annual audit plan coverage.

3. Conclusions

We conclude that, by using an integrated approach to risk assessment and risk management will be eliminated the need for a separate Internal Audit risk assessment over prevailing risks. It will reduce the level of risk assessment overlap by different functions over the same risk categories as a single methodology is used and will align timings of risk assessment exercises. The usage of the score method to prioritize the risks included in the annual audit plan is a useful and recommended tool in order to increase accuracy and timelines.
On the other side, we emphasize the recommendation that, each organization must develop its own risk management reporting manual/policy. The policy must clearly state the organization's commitment to the management of risk; the organizations have to identify risk owners to ensure accountability and authority. It must be clearly differentiate between those who are " accountable " for managing risk (those persons with a liability, either corporate or legal, for their decisions or lack of decision) and those who are " responsible " for specific tasks (those persons with an obligation to carry out an instruction from a competent authority). (ISO 31000:2009 Risk management –Principles and guidelines)

4. Bibliography

1. ISO 31000:2009, Risk management – Principles and guidelines; ISO Guide 73:2009, Risk management vocabulary; ISO/IEC 31010:2009, Risk management – Risk assessment techniques
2. Kevin W. Knight AM, "Future ISO 31000 Standard on Risk Management", *ISO Focus*, 2009
3. Maria Lazarte and Sandrine Tranchard, **"**The risk management toolbox**"**, *ISO Focus*, 2010

4. Duncan, W., R., "A Guide to the Project Management Body of Knowledge Guide**",** *Project Risk Management, Upper Darby,* 1996
5. Valentin P. Mazareanu, " Risk Management and Analysis: Risk Assessment (Qualitative and quantitative)", Analele UAIC Iasi, 2007
6. Mark T. Edmead, " Understanding the Risk Management Process", The Internal Auditor Magazine, The IIA, May 2007