Periodic risk assessment by internal audit

I Introduction

The Good Practice Internal Audit Manual Template, developed by the Internal Audit CoP of Pempal, defines the importance and the impact that an effective audit strategy and audit plan can have on meeting the overall goals, objectives and the mission of the internal audit unit. Planning provides a systematic approach to the internal audit work and requires knowledge and competency in a broad number of areas such as risk assessment and internal control.

This Risk Assessment Methodology Template elaborate more in detail the risk assessment process as described in paragraph 3.1.2 of the Good Practice Internal Audit Manual Template:

- Identification and definition of appropriate risks categories;
- Identification and definition of risk criteria for impact and probability;
- Definition of risk scoring content and an explanation of the rationale for assigning a score of high, medium or low to a particular riskThis template is based on the IIA Standard 2010 which says :

"The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals" and 2010.A1 requires–

"The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process".

While drafting the template also IIA advisory and guidance notes are used as well as generally accepted good practice adopted for such exercises.

The template follows the risk-assessment process step-by-step and gives for every step a practical example. In annexes more examples of used terminology can be found.

II Why is Risk Assessment an important part of Internal Audit?

The Head of an Internal Audit unit is responsible to develop a strategic and annual internal audit plan. These plans are developed through a process that identifies and prioritizes potential audit topics. The entire population of potential topics (which can

be operating processes or units) is called **the audit universe**[i1]. For each of these relevant topics within the audit universe the risks or opportunities will have to be assessed.

What are risks?

Risk is the possibility that an event will occur and adversely affect the achievement of an objective

Key risks are these risks that, if properly managed, will make the organization successful in the achievement of its objectives or, if not well managed, will make the organization fail.

Who is responsible for the risks?

Senior management of an organization is responsible to mitigate risks in a cost – effective way. As **'owners of the risks'** they have to set up a risk management system.

Risk management relates to preventing bad things from happening (risk mitigation), or failing to ensure good things to happen (pursuing opportunities). While many risks do present a threat to the organization, failure to achieve positive outcomes may also create an obstacle to the achievement of an objective and thus needs to be considered a risk.

The risks, and the way they are managed by the organization, should be independently assessed by internal audit. The results of this assessment will provide appropriate periodic audit coverage of a risk ranked audit universe.

Additionally, internal audit will capture the input from senior management to make sure that the prioritized risks are in line with management views and expectations.

When assessing risks?

The periodic risk assessment should ideally happen towards the end of the year, e.g. in November or December. However, any time when significant events occur, e.g. budget revision or radical cost cutting, risk exposures will change and a new (partial) risk assessment needs to be performed. The results of this renewed risk assessment may lead to changes in the annual internal audit plan.

III What is Process of Risk Assessment ?

[1] Explaining the process of defining the Audit Universe is not covered in this template but is the first step in the audit process. In this template it is considered as a given

Each organization will face different types of risk. Risk represents a range of possible outcomes, from the best to the worst case scenarios. The risk-assessment process consists of **five steps**.

Step1. There are an extensive number of risks that organizations face as they try to execute their strategies and achieve their objectives. Therefore it is wise to start with ***categorizing the risks***

Step2. Subsequently, one needs to define for every risk (sub)-category which risks are going to be assessed. This part of the risk assessment process is called ***defining risk-factors.***

Step3. Not every defined risk represents the same degree of threat to the organization. That's why is in step 3 Internal Audit assesses the impact of the risk and the probability of the occurrence of the risk. This part of the risk-assessment process is called ***defining the risk criteria*** in terms of how risks will be assessed and measured

Step4. Once the relevant risk factors and risk criteria have been defined they need to be assessed and scored. This step is called ***risk scoring***

Step5. The results of the assessment of the various relevant risks will be consolidated in the audit universe. This step is called ***defining a risk-ranked audit universe,*** which will be the basis for the development of multi-annual and annual internal audit plans

BOX VISUALISING STEPS

IV Steps of Risk- Assessment in detail

1. How to come to risk categories?

In order to categorize risks it is mandatory to follow a methodology to map and assess the various risks.

A good way to a structured approach to risk assessment is to allocate the risks to a select group of risk categories.

In the public sector it makes sense to identify the following broad categories:

- *Governance, strategy and planning*. This is the category of risks related to the way the organization has organized itself, including the development of its objectives, strategy and planning.

- *Operations*. These are the risks related to the key operations of an organization. As an example, for the Ministry of Education, this category will encompass the risks associated with the maintenance of schools, the recruitment of good teachers, the delivery of recognized diplomas, etc.
- *Infrastructure*. These are the risks related to the various supporting processes within the organization. Examples of supporting processes are human resources, information technology, finance, etc.
- *Compliance*. These are the risks related to legal and regulatory requirements. Examples of these risks are non-compliance with labor laws, fiscal requirements, health and safety regulations, etc.
- *Reporting*. These are the risks related to financial and operational, mandatory or requested, reporting. Examples are management declarations, financial statements, press releases, etc.

Because some categories may become very large, we may subdivide them in sub-categories. For example, we may divide the **category of Infrastructure** into the following sub-categories:

- *Human resources*. This sub-category may include recruitment, payroll, training, retirement program, performance and compensation, etc.
- *Information technology*. This sub-category may include IT infrastructure, change management, business continuity, information security, data protection and privacy, software licensing, etc.
- *Legal services*. This sub-category will include legal and regulatory matters, including contract management.
- *Finance* . This sub-category will include all budgeting, accounting and finance matters.

BOX WITH CASE EXAMPLE OF RISK CATEGORY

2. How to come to Risk factors?

Internal audit will have to develop a list of all potential and relevant risks based on input from management, information available within the organization, information from other assurance providers or information from peers. In practice, members of the internal audit function will interview the responsible leaders of the various organizational units (“risk-owners”) , whilst also looking at scientific publications and existing professional risk management and audit bodies, and at analyses of risks made by risk managers, etc.

Examples of risk factors are:

- Category “Governance, strategy and planning”.

    - Sub-category “Organizational structure”.
        - Risk 1: Unclear lines of authority
        - Risk 2: Complex organizational design
        - Risk 3: Excessive divisional focus
        - Risk 4: …
- Category “Infrastructure”.
    - Sub-category “Information security”.
        - Risk 1: Ineffective access controls
        - Risk 2: Vulnerability to malicious attacks
        - Risk 3: Lack of segregation of duties
        - Risk 4: …

BOX WITH CASE EXAMPLE OF RISK FACTORS

3. What are risk criteria in public sector organizations? .

Each organization should define criteria to be used to evaluate the significance of risk. The risk criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy, be defined at the beginning of any risk management process and be continually reviewed.

Risks are measured in terms of **impact and probability**. The impact defines the financial or non-financial consequences for the organization should the risk occur. The probability defines the chances that the risk may occur. The more vulnerable the organization is towards the mitigation of a specific risk, the higher the probability that the risk may occur.

The following **criteria for impact** may be considered:

- *Financial impact*. The monetary consequences for the organization should the risk occur.
- *Impact on reputation*. The consequences with regard to the reputation of the organization, minister or even at a higher level the reputation of the entire country in the eyes of rating agencies, international donors, etc.
- *Regulatory impact*. The occurrence of the risk may result in frozen budgets or programs or even in fines (e.g. EU funds) .
- *Impact on mission*. The mission of the organization may be impacted by the occurrence of the risk.

The following **criteria for probability or vulnerability** may be considered:

- *The effectiveness of the internal control system*. This can be assessed based on previous internal audit experience or on the existence / absence of major failures in the recent past.
- *The speed of response.* Not all risks may have an immediate impact of the organization. The speed of response determines the time that the organization has to respond to a risk when it occurs. The more time it has to remediate, the less vulnerable the organization is.
- *The complexity of the operations*. Complex operations are only understood by very few people within the organization. The less people understand the operations, the higher the chances that something wrong may not be noticed.
- *The rate of changes within the organization*. Stable systems and processes make the organization less vulnerable.
- *The capability of people and processes*. The more structured and transparent processes are, the less vulnerable the organization is. Less competent people make the organization more vulnerable.

The above criteria are just examples. The proper criteria need to be selected depending on the specifics of the organization. As a result, less or different criteria may be selected.

When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how probability will be defined;
- the timeframe(s) of the probability and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or tolerable; and whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

BOX WITH CASE EXAMPLE OF RISK CRITERIA

4. How to score the risks?

Once the relevant risks have been identified they need to be assessed and scored. It is recommended not to score the risks in a pure mathematical way. It is more practical to assess and score them according to a predetermined risk assessment grid. In the existing literature we often find three scoring levels, but this may lead to an over-scoring in the middle category. A risk assessment grid should ideally consist of **four scoring levels**:

- Low risk. Both impact and probability are assessed as low and not relevant.
- Medium low. Either impact or probability is assessed as a potential but not too relevant threat.
- Medium high. Either impact or probability is assessed as a potential and relevant threat.
- High. Both impact and probability are assessed as high and relevant.

People assess risks in different ways. Some people are by design risk averse and others are risk takers. If one person assesses a risk as high and the other as low, the result can never be medium. A consensus needs to be reached. Therefore it is recommended to agree upfront how risks are going to be scored, using a risk assessment grid.

BOX WITH RA GRID

A few examples:

- A risk may be considered to have a high financial impact if the occurrence of the risk may generate losses that are higher than 3% of the organization's budget.
- The reputation of the organization may be severely affected if the occurrence of the risk may generate national and international press coverage.
- The organization may be considered to be highly vulnerable if the occurrence of the risk affects a high number of transactions and/or processes.
- The organization may seem to be less vulnerable if the process controls are well designed and implemented, and operate effectively.

BOX WITH CASE EXAMPLE OF RISK SCORING