

Progress on Risk Assessment

.....continued

Ms. Albana Gjinopulli, MPA
Mr. Stanislav Buchkov



Introduction

- Good Practice Internal Audit Manual Template, developed by IA CoP, 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.

- Risk Assessment is a process used to assign a number or score to potential risk areas based upon specific factors related to auditee's operations, internal controls, and liability to the organization.
- Examples of specific risk factors used to formulate the risk assessment model include the amounts of budgeted expenditures, complexity of transactions, time since last audit, compliance with laws and regulations.
- *The complete list of risk factors and RA process will be described further in the methodology.*

- The development of Internal Audit Plan, using the risk assessment model as an integral component, is a dynamic process.
- The Internal Audit Unit should have access to current information about departments to use in the risk assessment process on an ongoing basis.
- The risk factors and scoring process will be reviewed and refined periodically as needed.

The purpose of RA Methodology

- The main purpose of the Risk Assessment Methodology is to provide **for** an objective and transparent basis for the preparation of Audit Plan.
- The purpose of Risk Assessment is for internal audit to give priority to higher risks for the organization.
- *Therefore, the risk assessment methodology is one of the cornerstones of the internal audit activities.*

- The risk assessment process shall be described in detail and should cover:
 - Identification and definition of appropriate risk 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 risk.

Definitions of Risk Assessment

- Risk is an uncertain future event which could adversely affect the achievement of an organization's objectives.
- Risk likelihood- is the probability that a risk occurs. The factors that should be taken in the determination of the likelihood are: the source of the threat, capability of the source, nature of the vulnerability and existence and effectiveness of current controls.

- Likelihood can be described as: high- an event is expected to occur in most circumstances; medium- an event will probably occur in many circumstances and low- an event may occur at some time;
- Risk impact- is the potential effect that a risk could have on the organization if it arises. The magnitude of impact can be categorized as: high- serious impact on operation, reputation, or funding status; medium- significant impact on operations, reputation or funding status and low- less significant impact on operations, reputation or funding status.

Steps undertaken



- Establishment of working group in Ohrid
 - Development of survey
 - Analysis of survey results
 - Development of final objectives of working group
- Development of action plan



Establishment and Composition of Risk Assessment Working Group



- Albana Gjinopulli, leader
- Stanislav Bychkov, co-leader
- Joop Vrolijk, OECD/SIGMA
- Jean-Pierre Garitte, OECD/SIGMA expert
- Other members of IA COP

Objectives and results to be achieved.....

- Inventorize current practices
- Develop good practice model
- Develop good practice guidance, *which can be used by various countries as a basis for their risk assessment*



Next steps.....work to be done

- Develop content of each topic to be included in the model (*between June and October 2012*)
- Expose draft model to members of the IA COP (October 2012)
- Discuss draft and comments in next meeting of RAWG (*plus ongoing discussion*)



Develop Good Practice Risk Assessment Template (*January and on going*)

Intermediate results, Consolidation of inputs



| Components | | Pink | Red | Orange | Green | Yellow |
|--|--|------|-----|--------|-------|--------|
| Purpose of risk assessment | | √ | √ | √ | √ | √ |
| Objective of template | | √ | √ | | | |
| Standards | | | √ | | | |
| Objectives of the organization | | √ | √ | √ | √ | √ |
| Strategic objectives | | | | √ | √ | |
| Specific objectives | | | | √ | √ | |
| Role of internal audit with regard to objectives | | | | √ | √ | |
| Audit universe | | √ | √ | √ | √ | |
| Processes (owners) | | √ | √ | √ | | |
| Risk owners | | | | | | √ |
| Priority processes to be audited | | | | √ | | |
| Risk definition | | | | √ | | |

Table of Content

I. Introduction

II. Purpose and Principles of Risk Assessment

III. Objectives of the organization and Audit Universe

Strategic objectives

Specific objectives

Role of internal audit with regard to objectives

IV. Process of Risk Assessment

IV.1 Definitions of Risk

IV.2 Objective of Risk Assessment

IV.3 The process

IV.4 Risk factors

V. Types of risk (categories)

VI. Risk identification

VI.1 Source of information

VI.2 Techniques to gather information

VII. Risk assessment

VII.1. Inherent risk, residual risk

VII.2. Criteria for risk assessment

VII.3. Classification

VII.4 Risk scoring

VII.5 Risk rating

VII.6 Risk matrix

VII. Processes (owners)

Risk owners

Priority processes to be audited

VIII. Addressing risk assessment

VIII.1. Prioritization

VIII.2 Frequency of audits

VIII.3 Coverage with resources

IX. Validation of risk assessment results

X. Documentation of risk assessment in audit plan

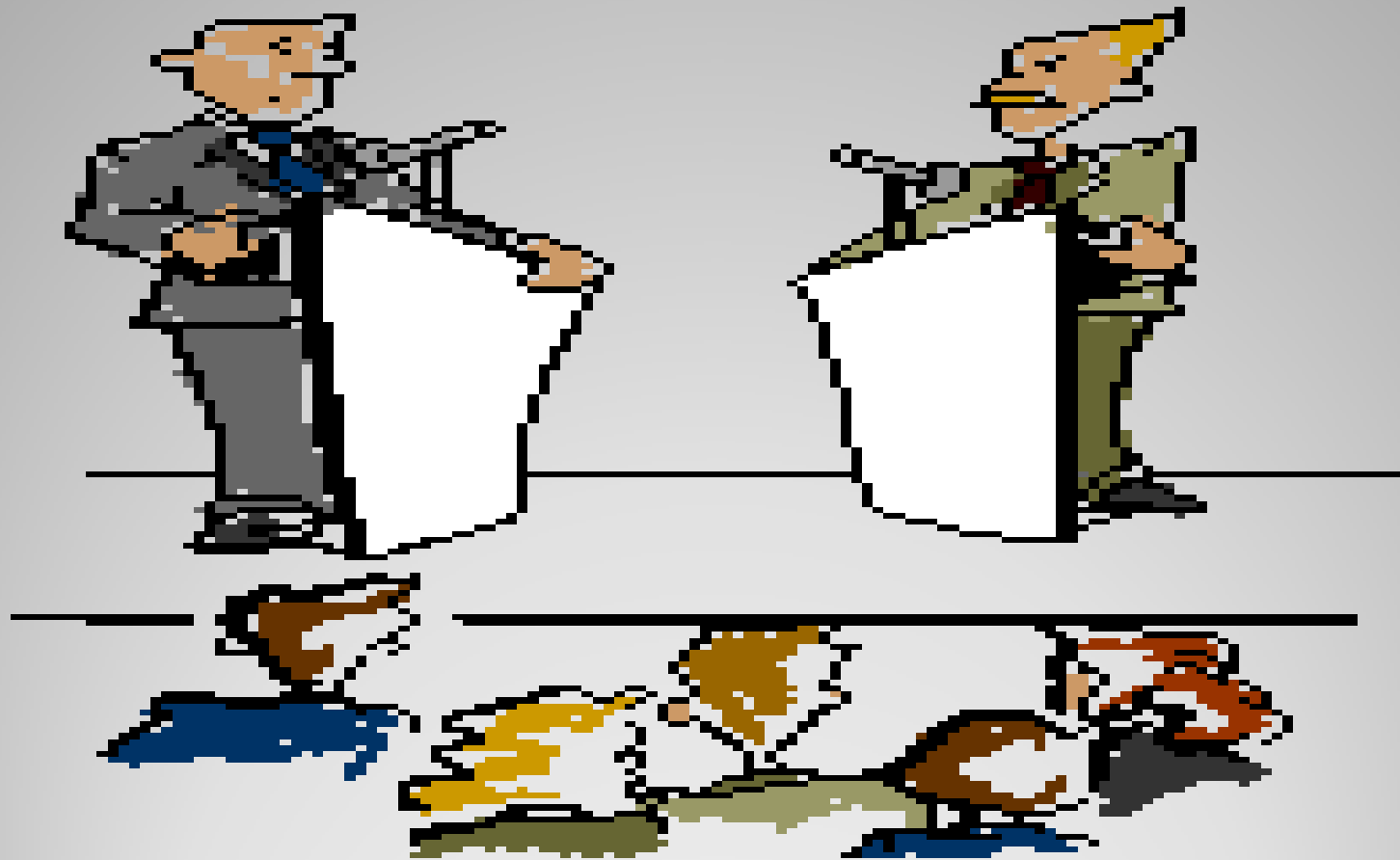
XI. Monitoring process of Risk Assessment

ANNEXES

Annex 1: Risk Assessment questionnaire

Annex 2: Practical examples of risk factors scores and weight

Annex 2: Glossary of terms



Thank you for the attention....

- Take a deep dive into one process: identify sub-processes.
- Identify risk categories applicable to MoF.
- Identify risk criteria for impact and probability (or vulnerability).
- Identify risk scores (plus explanation) for selected sub-process.

What needs to be done?