RISK ASSESSMENT TEMPLATE

Where are we now?

What have we prepared?

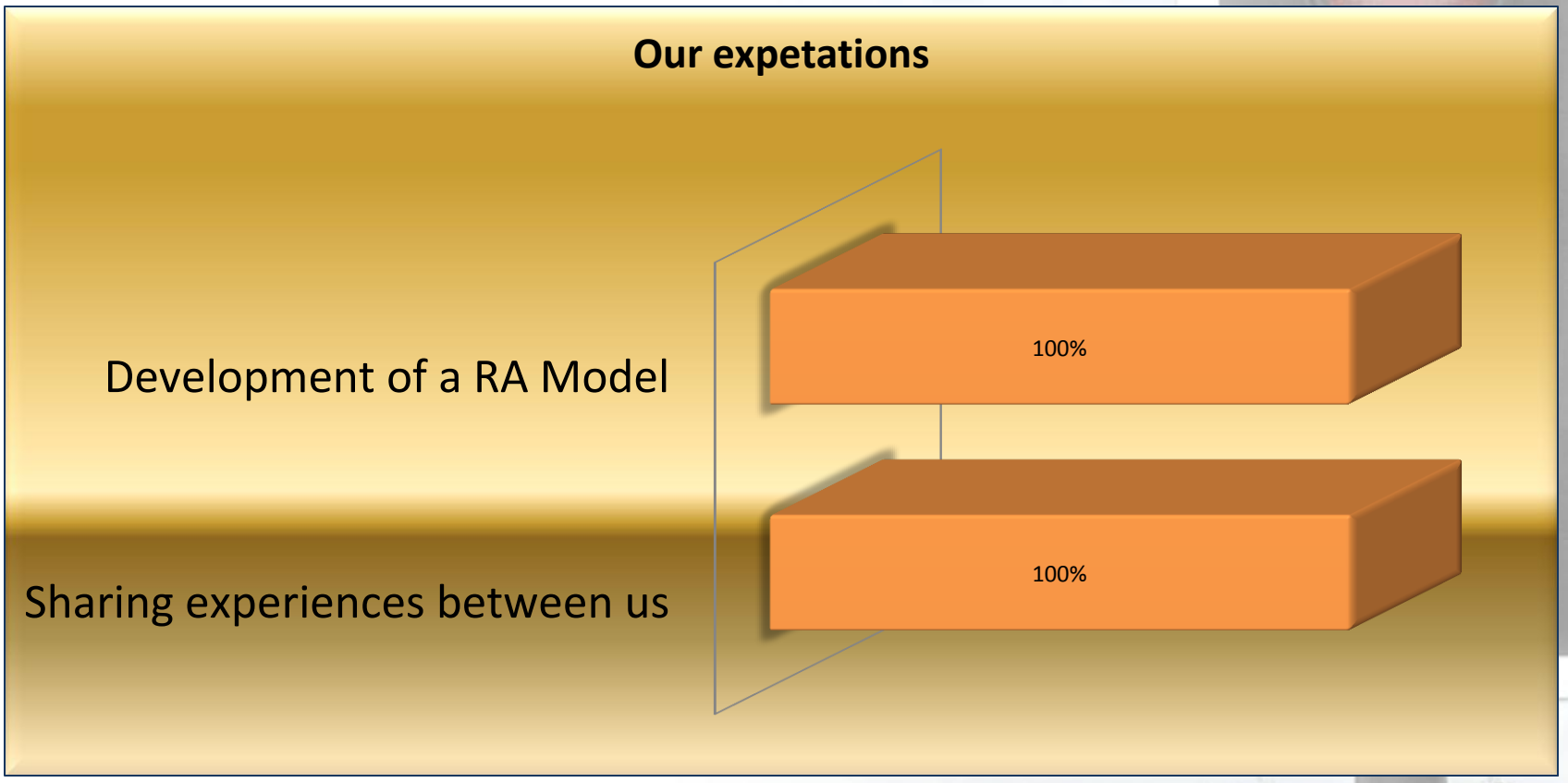
PEMPAL IA-CoP Workshop Risk-Assessment, Tirana, Albania, 28-30 January 2013

Albana Gjinopulli
Joop Vrolijk

Why did we took the initiative for a Risk Assessment Template?

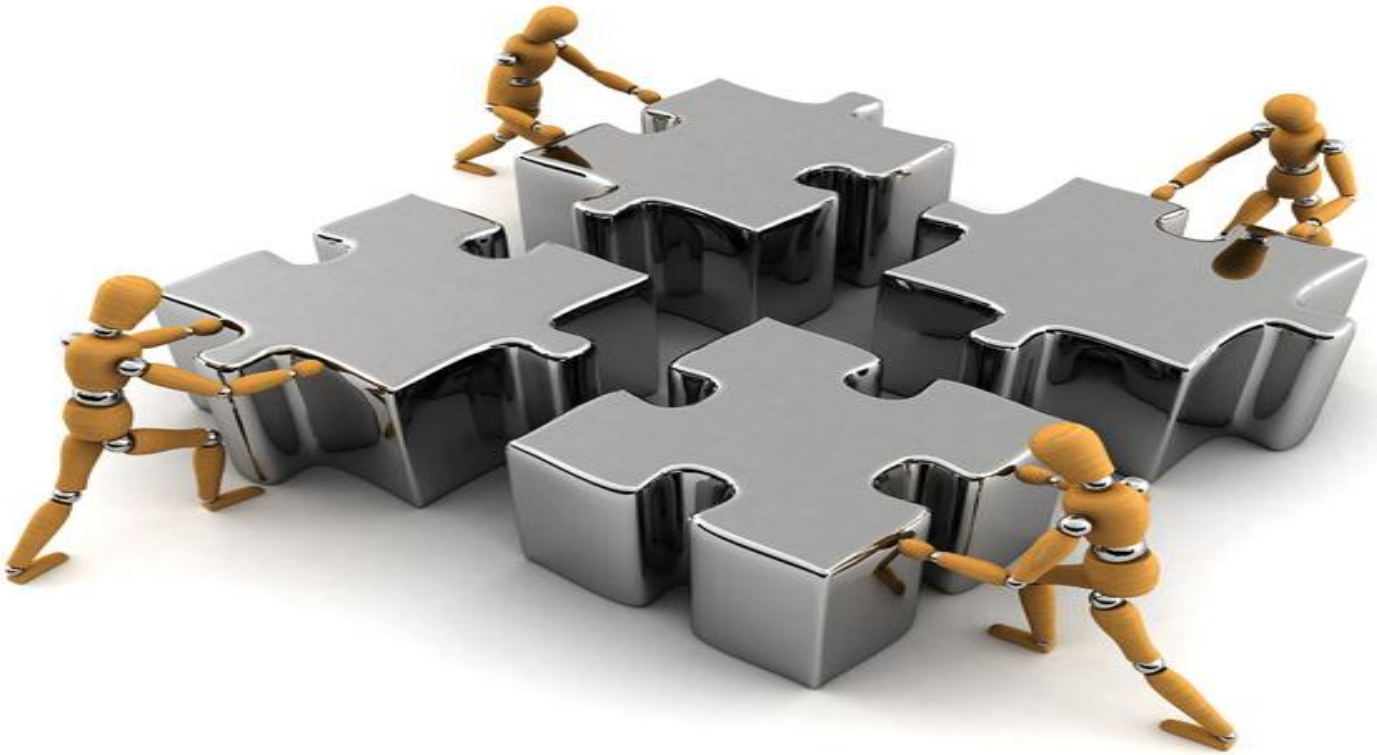
- Topic was identified as the most requested by IA CoP, Ohrid, Ocrober 2011
- Results of questionarie presented in Sofia, April 2012
  - Some countries have dveloped a methodology for RA (as part of IA Manual or separately)
  - In other countries it is very vague or it is missing at all
  - In both cases, RA is not really implemented in practise

What are the expectations of RA workshops?



Our Objective?

Work together on developing a RA Model Template



QUESTIONS addressed in RA Template

topic

- Importance of RA
- What are risks

topic

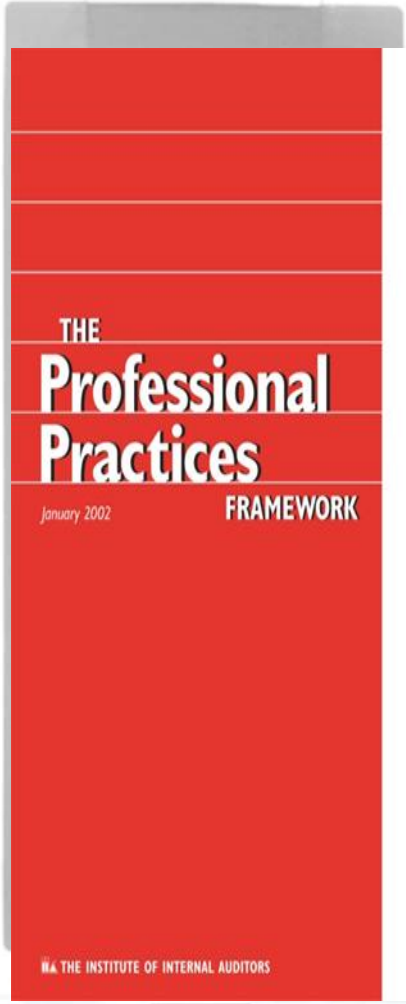
- Risk's owners
- When assessing the risks
- The process of RA

topic

- Risk Categories
- Risk Factors
- Risk Criteria
- Risk Scoring

My Boss asked me :Why do internal auditors assess the risks?

- **2010.A1** – The internal audit activity's plan of engagements should be based on a risk assessment, undertaken at least annually.
- **2120.A1** – Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems.



Only because the Standards say that??? Are they mandatory????

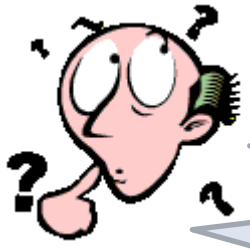
- No .... is advised by IIA but offers multiple advantages:
- For annual audit planning
  - ✓to target high impact areas
  - ✓to allocate our scarce resources

What else.....

- When planning/executing audits
  - ✓frame objectives
  - ✓establish scope
- When providing consulting services
- To advise management
  - ✓on vulnerabilities
  - ✓on corrective actions

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 resposible 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.

Remember!

"Management is responsible for identifying risk and for the internal control environment…When an organization has a standard risk assessment framework in place, the internal auditor can draw on this…When there is no such framework, the internal auditor's work will provide valuable information about the organization's risk to top management."

Source: A Guide to the Use of Risk Management Within the Internal Audit Process

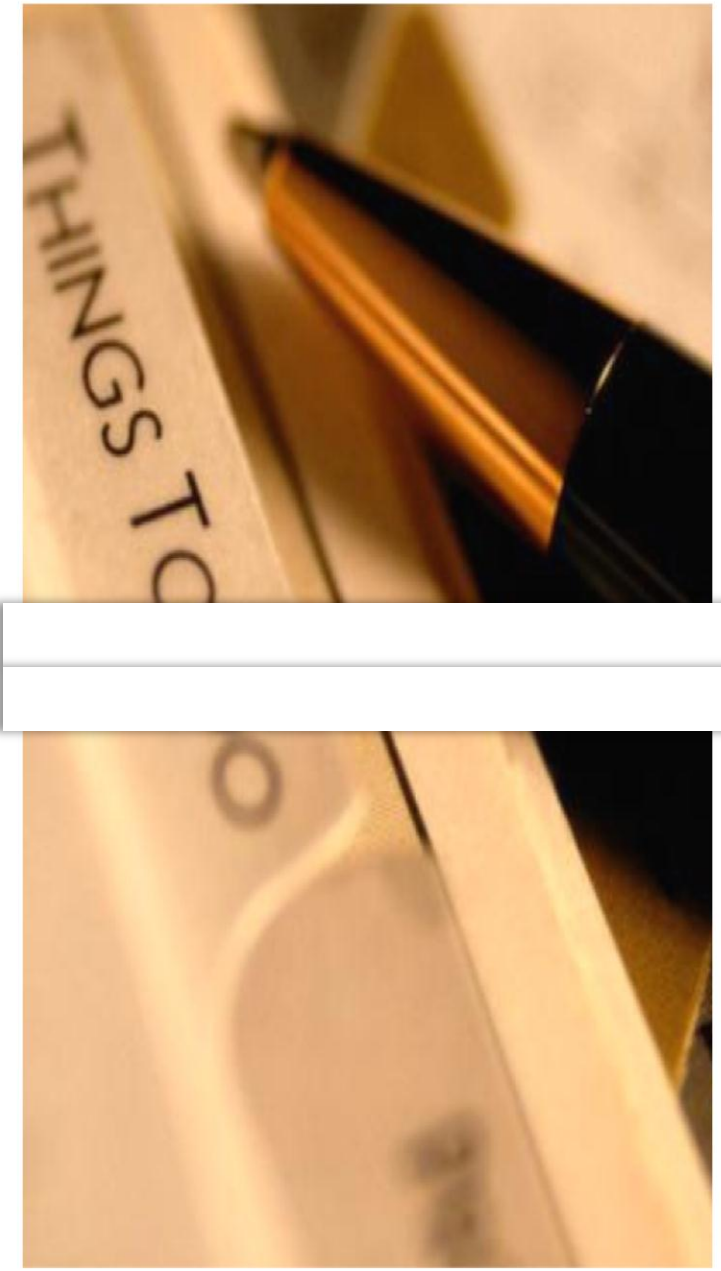
Risk Management

- 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.

Risk Assessment

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.



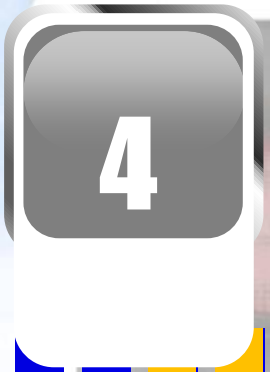
Risk management: The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk assessment: A *systemic process for assessing and integrating professional judgments about probable adverse conditions and/or events*.

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

Process Flow /5 Stages of RA



Categorizing Risks

There are an extensive number of risks that organizations face as they try to execute their strategies and achieve their objectives.

Risk Factors

Subsequently, one needs to define for every risk (sub)-category which risks are going to be assessed.

Risk Criteria

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.

Risk Scoring

Once the relevant risk factors and risk criteria have been defined they need to be assessed and scored

Risk-Ranked Audit Universe

The results of the assessment of the various relevant risks will be consolidated in the audit universe

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

Main 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.

Other Risk Categories

•**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.

Sub Categories, e.g the category infracture:

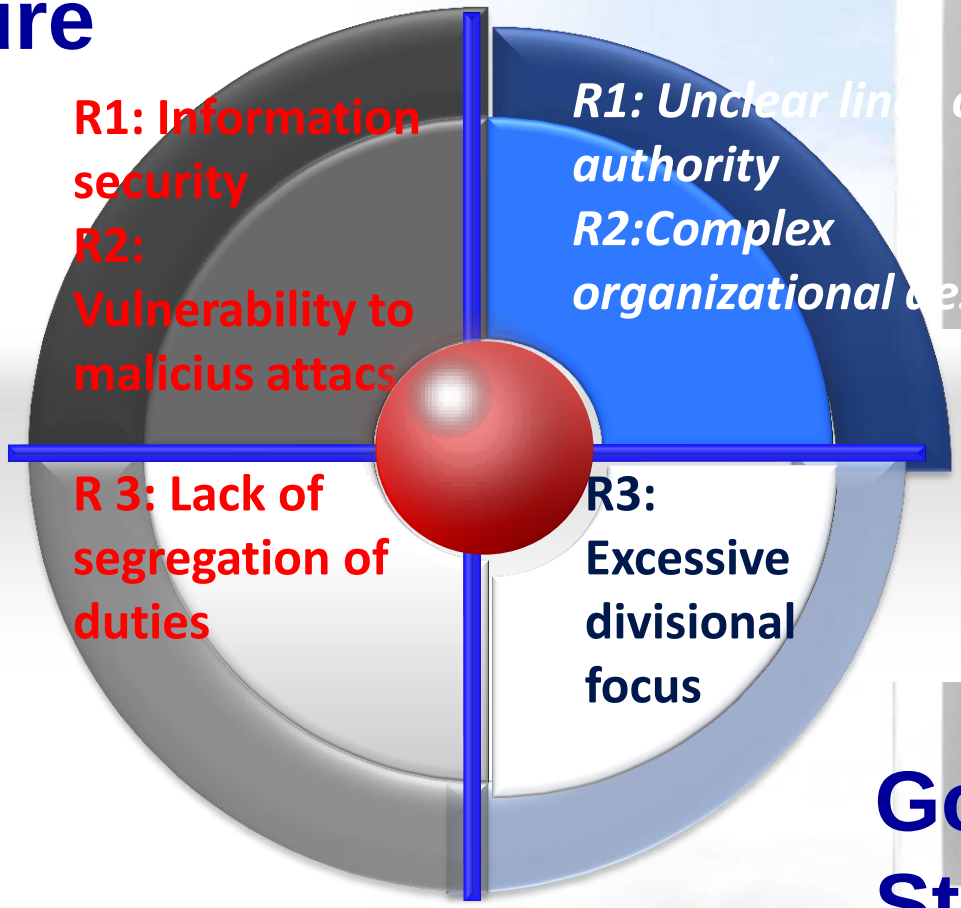
- **Human resources.** This sub-category may include recruitment, payroll, training, retirement program, performance and compensation, etc.
- **Information technology**. This sub-category may include IT infrastructure, change management, business continuity, information security, data protection and 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.

What about 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 per Sub-Category

Infrastructure



Governance, Strategy and Planning

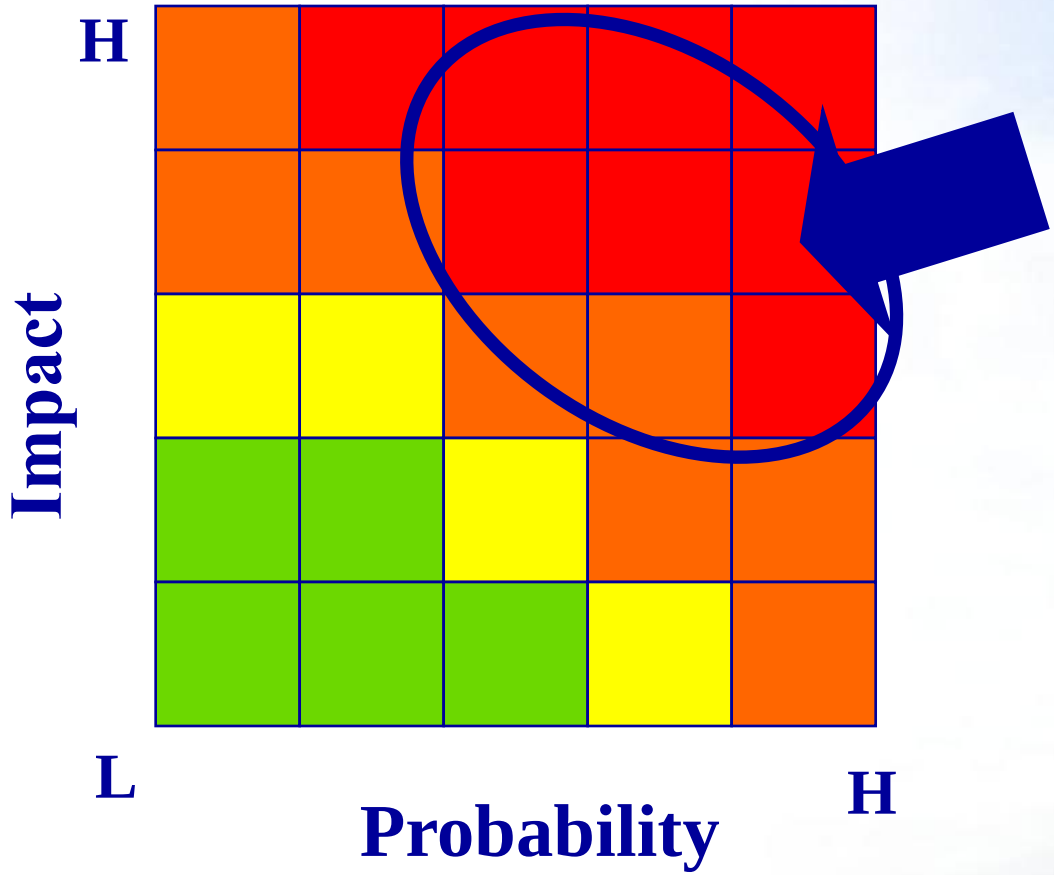
What are risk criteria in public entities?

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.

Impact and Probability

- 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 Objective of Risk-Based Planning



Target audit resources where risk is greatest!

But .....audit periodically lower risk level units/processes

Source: A Guide to the Use of Risk Management Within the Internal Audit Process

Criteria for impact

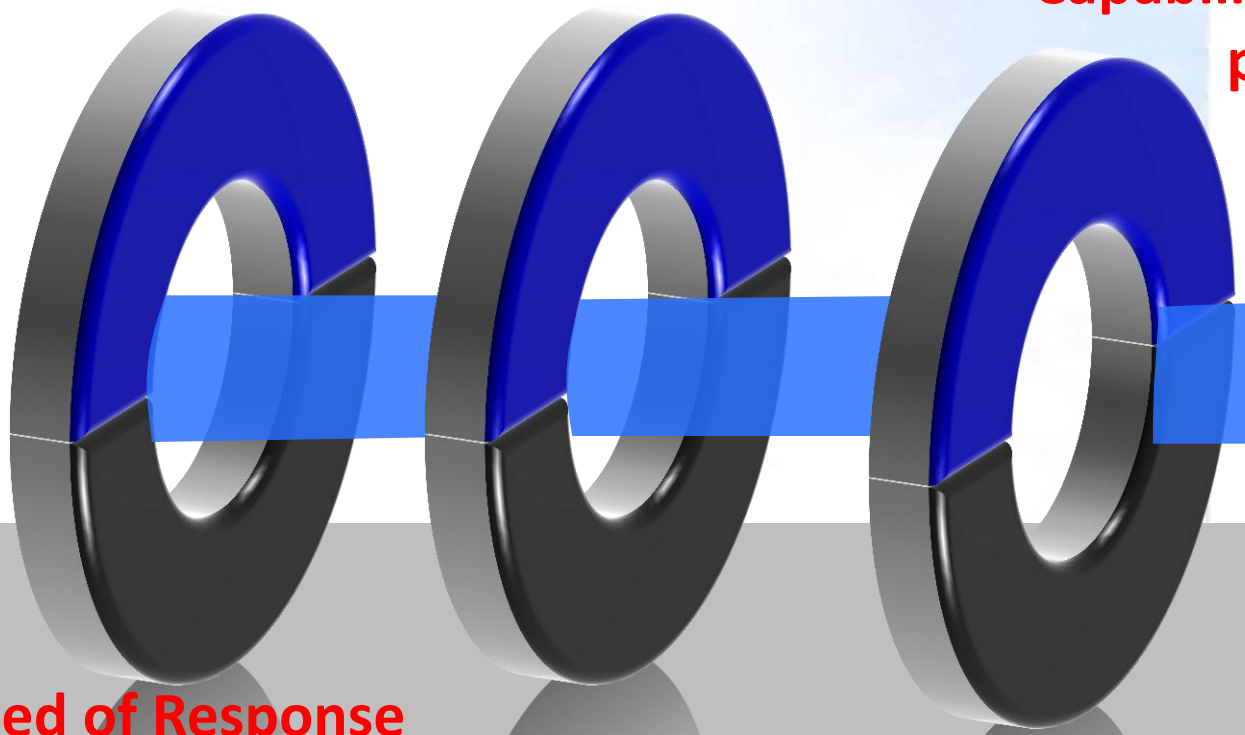
Impact:
Low
Medium Low
Medium High
High

Criteria for probability

The effectiveness of the internal control system

Complexity of operations

Capability of people and processes



Propability:

Low

Medium Low

Medium High

High

Speed of Response

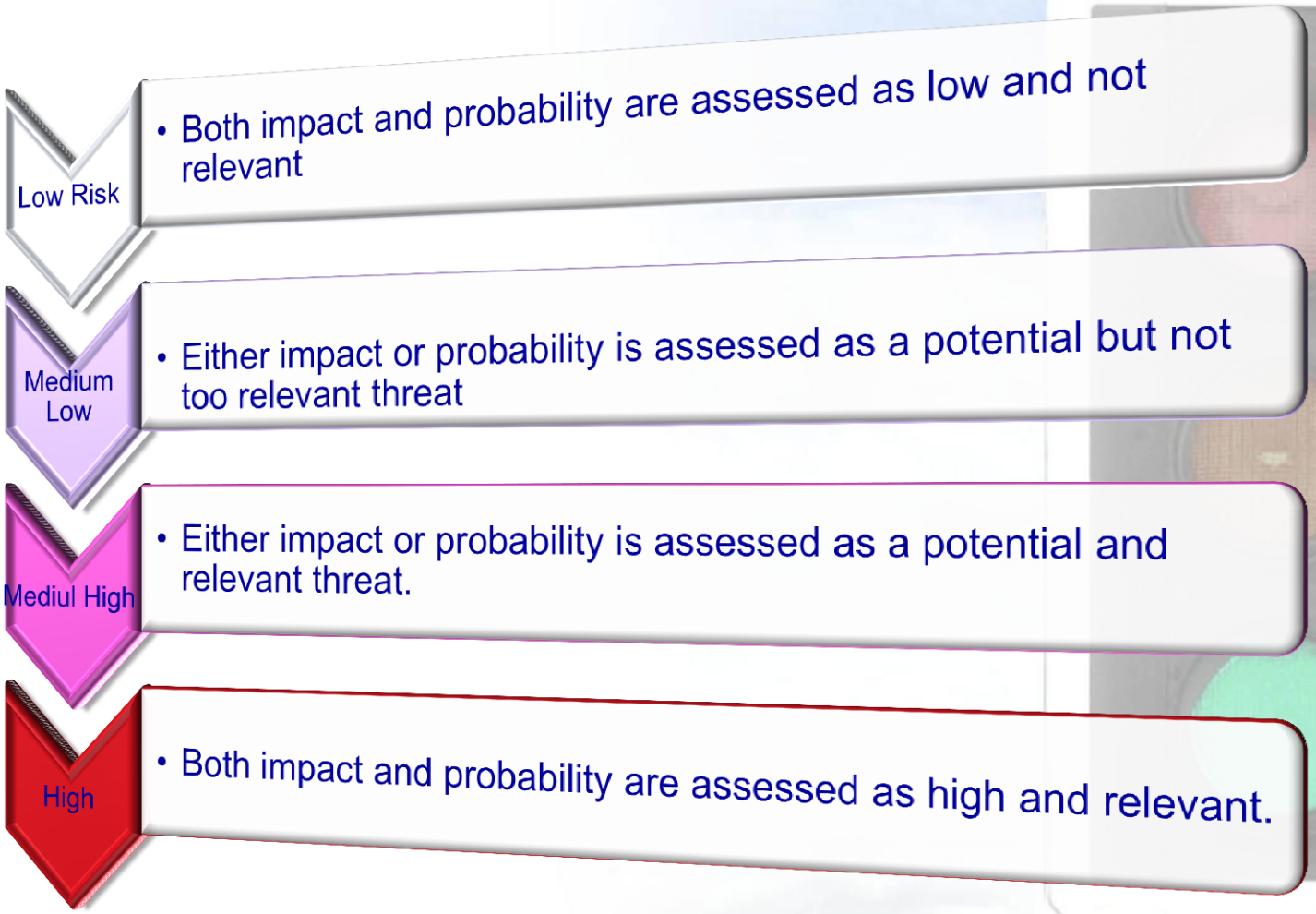
Changes within organisation

LOGO

Risk's Scoring.....

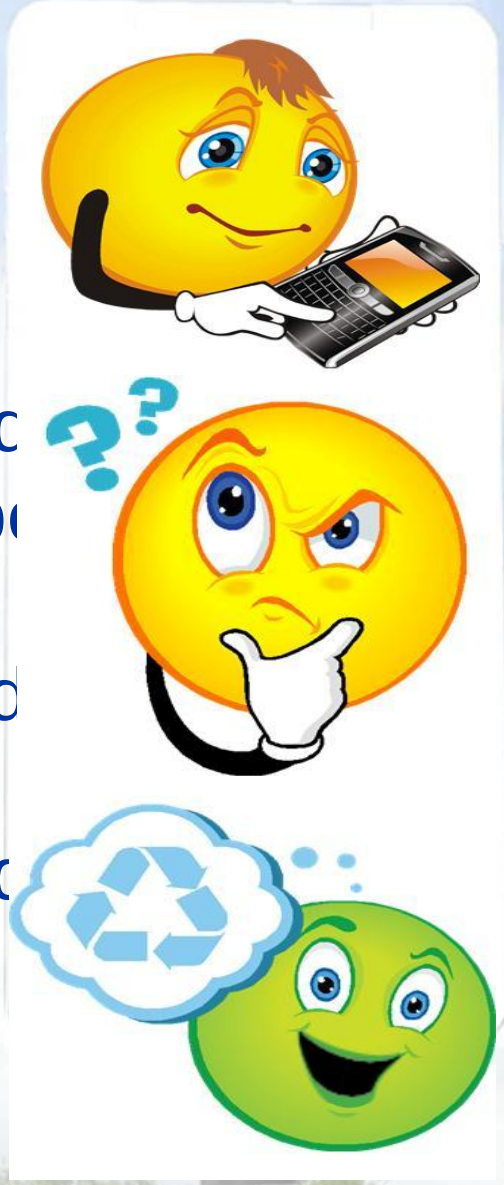
Once the relevant risks have been identified they need to be assessed and scored. It is recommended not to score the risks in a pure mathematical way. It is more practical to assess and score them according to a predetermined risk assessment grid. In the existing literature we often find three scoring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

A risk assessment grid should ideally consist of four scoring levels:



Risk Appetite

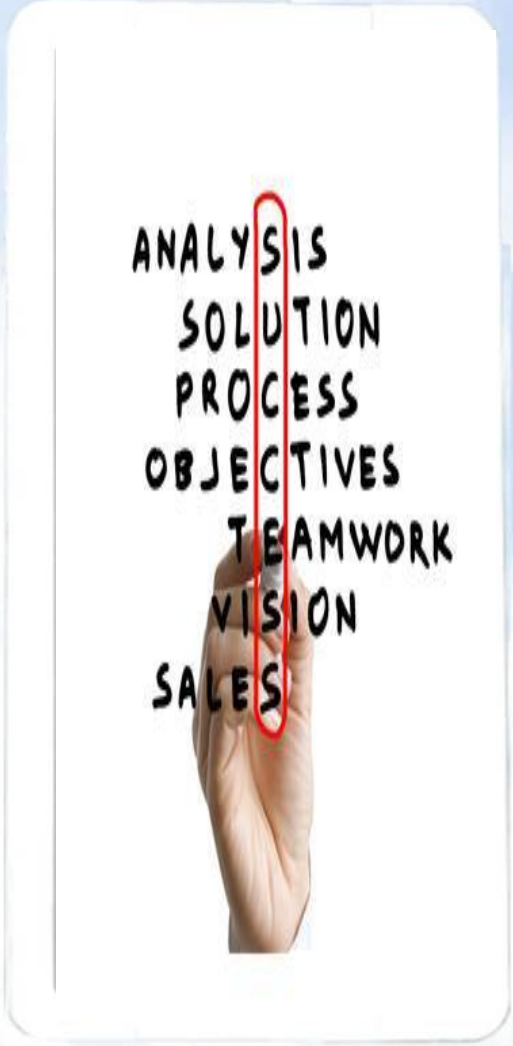
- People assess risks in different ways. Some people are **by design risk averse** and **others are risk takers**. If one person assesses a risk as high and the other as low, the result can never be medium. A consensus needs to be reached!!! Therefore it is recommended to agree upfront how risks are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



The process is SUBJECTIVE and based on PROFESSIONAL JUDGMENT!!

Integrating RA Results

- 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



Then.....

- Use the information collected, take into account the risk matrix and draft your audit plan;
- Consult with Executive Management and finalise Audit Plan;
- Make adjustments if necessary- making sure that the plan is realistic and all relevant informaion is considered

Obtain Approval

Publish the organization's annual audit plan


It's QUESTION TIME !!