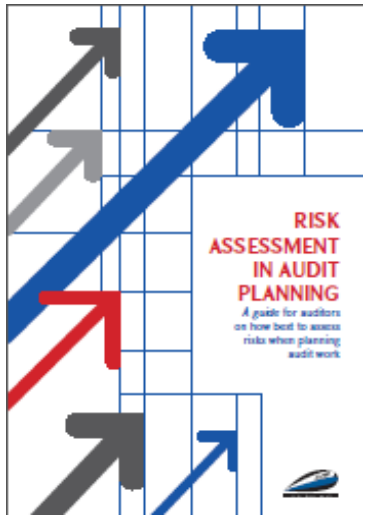
INTERNAL AUDIT COMUNITY OF PRACTICE FOR INTERNAL AUDIT

IA COP
INTERNAL AUDIT
COMMUNITY OF PRACTICE

Public Expenditure Management
Peer Assisted Learning

Strategic and Annual Internal Audit Planning

PEMPAL IACOP Good Practice “Risk Assessment in Audit Planning”



Content

- Introduction
- Glossary
- Risk based audit planning vs. Risk management
- Risk based audit planning stages
  - Audit universe
  - Risk identification and assessment
  - Developing generic risk factors and criteria
  - Developing and maintaing strategic and annual plans

Introduction

- Working group established in 2012
- Objective
  - to understand risk management and risk based audit planning
- Final product - Risk Assessment in Audit Planning Guide (2014)
  - 5 chapters
  - Annexes

Introduction

- **Standard 2010 Planning**

- The chief audit executive must establish a risk based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

- ***Interpretation***
  - To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains the understanding of the organization's strategies, key business objectives, associated risks, and risk management processes.
  - The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.
- 2010.A1
  - The internal audit activity 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.

Glossary

- Event
  - an incident or occurrence, from sources internal or external to an organization, which may affect the achievement of objectives
  - events can have negative impact, positive impact or both. Events with negative impact represent risks
  - events with positive impact represent opportunities
- Risk
  - the possibility that an event will occur and adversely affect the achievement of objectives
  - risk is measured in terms of impact and likelihood
- Opportunity
  - the possibility that an event will occur and positively affect the achievement of objectives

Glossary

- Key risks
  - are these risks that, if properly managed, will make the organisation successful in the achievement of its objectives or, if not well managed, it (the organisation) will not achieve its objectives
- Inherent risk
  - the level of risk before any risk mitigation actions such as control activities have been taken into account (e.g. the inherent risk of flooding before taking into account flood prevention measures)
- Residual risk
  - the level of risk after taking into account risk mitigation actions such as control activities. The auditor is most concerned with the level of residual risk. (In some cases inherent and residual risk will be the same. But areas that are well controlled will usually have lower levels of residual risk.)

Glossary

- Risk appetite
  - the level of risk that an organization is willing to accept in pursuit of its objectives
- Risk factors
  - a term used to describe generic factors that can indicate a higher level of risk and/or priority to be given to one element of the audit universe

Risk based audit planning vs. Risk management

- Risk management
  - an integral part of internal control system
  - the responsibility of management
  - a structured process where managers
    - examine likely future events and the risks and opportunities these represent to the achievement of organization's objectives
    - determine and implement risk management actions (e.g. control activities)
- Internal audit risk assessment
  - part of planning process where auditors consider
    - individual events and the risks and opportunities these represent to the achievement of the objectives of elements of the audit universe
    - generic risk factors that help prioritize work to areas of highest risk

Risk based audit planning vs. Risk management

- The objective of risk based audit planning is to ensure that the auditor examines subjects of highest risk to the achievement of the organisation's objectives

- The auditor must assess risks to the achievement of the organisation's objectives even if management do not

- Risk based audit planning stages
  - risk management in place
  - no risk management in place

Risk based audit planning vs. Risk management

- If there is no risk management in place
  - **it is helpful to carry out a joint risk assessment workshop with management** and this could also include a short training session on risk management
  - this may also encourage management to develop their own risk management processes

Internal Audit Community of Practice

Risk based audit planning vs. Risk management

	Risk based audit planning	Risk management
Who responsible for the process?	Internal auditors	Management
What is the purpose of the process?	To decide on the focus of internal audit activity	To manage risk in order to achieve the objectives
What is the result of the process?	Risk based strategic and annual audit plan	Risk inventory, Risk map, Action plan for managing risks
What are the steps?	A – if there is a risk management in place – IA use the information from it, but still use their own professional judgement B – if there is no risk management in place – with the involvement of management IA should assess the risks by their own in order to establish audit plans, but this risk assessment cannot be considered as risk management!	1. Risk identification 2. Risk analysis 3. Risk evaluation 4. Decision on how to manage the identified risk (Determination of Risk appetite, choosing the strategy for risk mitigation) 5. Action plan 6. Take action to mitigate risks 7. Monitoring of action plan

Risk based audit planning stages

1. Determining and categorizing the audit universe

2. Risk identification and assessment

3. Developing generic risk factors and criteria for each factor to identify the audit priority of audit objects within the audit universe

4. Developing and maintaining risk based audit plans (strategic plan and annual work plan)

Audit universe

» The IA CoP's Good Practice Internal Audit Manual template

» *"The overall scope of the internal audit function and the totality of auditable processes, functions and locations"*

» The phrase "audit universe"

» a simple way of referring to all the totality of all things that an internal auditor could separately examine

Audit universe

- Head of IA has to decide how to categorize the audit universe and how many slices it makes sense to use. Most IA units will therefore want to consider the following as the minimum categorizations needed:
  - *By organisational structure*
  - *By common processes*
  - *By location*
  - *By operational programmes*
  - *By service lines*

- Possible information sources for categorizing the audit universe:
  - *Management information giving a breakdown of goals, objectives and targets*
  - *Guides to the organisation's services*
  - *Organisational charts or office directory*
  - *Annual reports and any performance targets set for the organisation*
  - *Corporate and departmental plans, business plans*
  - *Development plans for IT, other infrastructure and buildings*
  - *Budgets*
  - *External audit and consultancy, inspection and review reports*
  - *Existing operational and strategic audit plans*

Risk identification and assessment

- Identifying risks
- Assessing risks in terms of impact and probability
  - Criteria for assessing impact
  - Criteria for assessing probability
- Scoring risks for impact and probability
- Combining assessment criteria into a risk matrix

Risk identification and assessment
Criteria for assessing impact

Level (score)	Example of scoring impact criteria		
	Financial	**People**	**Operations**
Low (1)	Financial impact is less than xxx,xxx.	Unplanned loss of several employees within a unit that may cause some disruption to the unit's operations.	Limited and minimal loss of operations. Promptly recoverable service interruption.
Medium (2)	Material financial impact that is more than xxx,xxx but less than xxx,xxx.	Unplanned loss of several key personnel in one unit that causes significant disruption to the unit's operations.	Significant loss in operations but restricted to a limited number of services/locations of the organization. Promptly recoverable service interruption.
High (3)	Material financial impact that is more than xxx,xxx but less than xxx,xxx.	Unplanned loss of several key personnel that causes significant impact in the operations of one or more departments.	Important loss in operations but restricted to a limited number of services/locations of the organization. Slow systems recovery.
Very High (4)	Significant material financial impact that is more than xxx,xxx.	Serious injury/death to personnel.	Organizational wide inability to continue normal business. Significant loss of operations. Widespread service interruption. Slow systems recovery.

Risk identification and assessment
Criteria for assessing vulnerability

Level	Criteria	Score
Rare	Event extremely unlike to happen	1
Unlikely	Event has remoote possibility of occurence	2
Medium	Event fairly likely to happen sometime in the future	3
Likely	Event will likely occure (within 1-2 years)	4
Expected	Event is already occuring or expected to occur	5

Risk identification and assessment
Risk matrix

Rare/ Improbable Unlikely 1 2			PROBABILITY				
			Medium	Likely	Frequent/ Expected		
			3	4	5		
IMPACT	Low	1	Low	Low	Low	Low	Low
	Medium	2	Low	Low	Medium	Medium	Medium
	High	3	Low	Medium	Medium	High	Very High
	Very High	4	Medium	High	High	Very High	Very High

Developing generic risk factors and criteria

- There is likely to be a high number of possible audit objects and a large number of risks, most auditors use a set of generic "**risk factors**"
  - to review the importance of each element of the audit universe to determine the priority that should be attached to each auditable object

- *Risk factors* - could also be described as *selection factors*
  - the purpose is to select the most appropriate audits to undertake

nature (control environment/vulnerability, sensitivity and management concerns).

Developing generic risk factors and criteria
Risk factors - scoring

Example of scoring risk factors Each of the risk factors is awarded a points rating on a scale of 1-5 as explained below.		
Element	**Description**	**Score**
A Materiality	System accounts for less than 1% of the annual budget	0
	System accounts for 5-10% of the annual budget	2
	System accounts for 25-50% of the annual budget	3
	System accounts for at least 75% of the annual budget	5
B Control environment/ Vulnerability	Well controlled system with little risk of fraud or error	0
	Reasonably well controlled system with some risks of fraud or error	3
	System with history of poor control with high risk of fraud or error	5
C Sensitivity	Minimal external profile to the system	0
	Potential for some external embarrassment if the sys- tem is not effective	3
	Major public relations or legal problems is the system is not effective	5
D Management concerns	System with low profile across the organization that has little impact on the achievement of business objectives	0
	System with high profile in recent past with a number of concerns for management due to recurrent failures	5

Developing generic risk factors and criteria
Risk factors - weighting

Example of weighting risk factors

Step 1 Each of the risk factors is given a weighting using judgement of the relative im- portance of each of the risk factors.

Element	Weighting
A Materiality	3
B Control Environment /Vulnerability	2
C Sensitivity	2
D Management concerns	4

Step 2 The factor score and weightings are then combined into a formula, which can be used to calculate the risk index.

Risk index = (A x 3) + (B x 2) + (C x 2) + (D x 4)

Step 3 Each audit object is then categorised as Very High, High, Medium, or Low risk- based on a suggest risk index score for example:

Risk Index Score	Risk/Priority
Over 45	Very High
40-45	High
30-40	Medium
Below 30	Low

It would be relatively easy to modify this system for use with a wider range of risk factors. More or fewer risk factors would require a different risk index score for very high, high, medium and low categories.

Developing and maintaing strategic and annual plans

Internal auditors consider how to develop strategic and annual plans and how to keep them up to date.

» Strategic plan

- » ***a "shop window" for internal audit***
- » *an opportunity to present to management all the things that an IA unit could do to help the organization achieve its objectives*

» Annual plan

- » *translates the strategic plan into the audit assignments to be carried out in the current year*
- » *should define the purpose (title and objectives) and duration of each audit assignment and allocate staff and other resources*

Developing and maintaing strategic and annual plans

- Keeping plans up to date
  - Regular monitoring of risk
- Annual review of the strategic plan
  - Updating Risk assessment each year
  - Considering significant events arising during the year
- Dealing with additional requests for audits during the year
  - Informing managers on the impact of undertaking additional audits during a year
  - Explaining what we will not do if we take on a new assignment