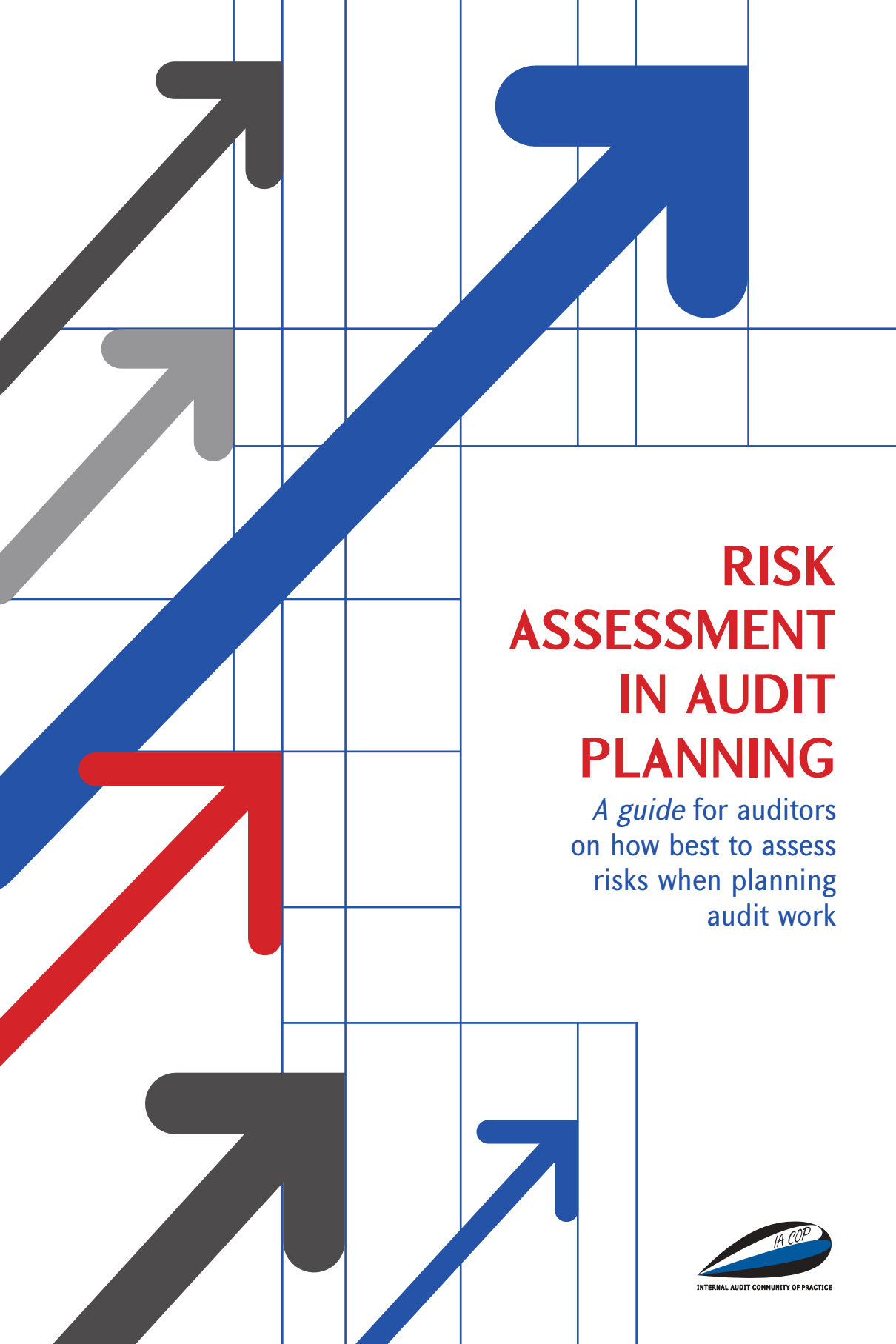


RISK ASSESSMENT IN AUDIT PLANNING

A guide for auditors on how best to assess risks when planning audit work

IA COP

INTERNAL AUDIT COMMUNITY OF PRACTICE

RISK ASSESSMENT IN AUDIT PLANNING

A guide for auditors on how best to assess risks when planning audit work

April 2014

Contents

Preface

This template is the product of a process of exchange of ideas and information among members of the Internal Audit Community of Practice (IA CoP), of the Public Expenditure Management Peer-Assisted Learning (PEM-PAL) network.

The PEM-PAL network, launched in 2006 with the help of the World Bank, is a regional body that aims to support reforms in public expenditure and financial management in twenty one countries in Central Asia and Central Eastern Europe by promoting capacity building and exchange of information. IA CoP, one of the three Communities of Practice around which the network is organized, has representatives from 21 countries of the Europe and Central Asia region.

One of the IA CoP's goal is to "contribute to improved Public Financial Management (PFM) systems, by supporting members to establish a modern and effective Internal Audit Service in their Governments that meets international and European Union (EU) standards and facilitates good governance in their public sector..."[1] IA CoP activities contribute to further this agenda by offering a guide in risk assessment in audit planning, which public sector internal auditors may follow as a good practice.

This Risk Assessment in Audit Planning guide is the end result of a collaborative process from regional members and donor partners, which began with a workshop held in Lvov, Ukraine in October 2012. It is the hope of the PEM-PAL network and IA CoP that users of this guide, and other documents in the series, will find them informative and useful in advancing the reforms of public sector internal auditing.

1 Source: IA CoP Balanced Scorecard

Acknowledgement

This template was the combined effort of a number of individuals and members of the Risk Assessment Working Group of the Internal Audit Community of Practice (IA CoP) who shared their time and expertise to make it a reality.

Specially, IA CoP would like to recognise the following key contributors:

Stanislav Bychkov, Russian Federation, Co-leader of Working Group on Risk Assessment

Ruslana Rudnitska, National Academy for Finance and Economics, the Netherlands

Richard Maggs, World Bank, Consultant

Manfred van Kesteren, National Academy for Finance and Economics, the Netherlands

Grigor Aramyan, Armenia, Leader of Working Group on Risk Assessment

Edit Németh, Hungary, Co-leader of Working Group on Risk Assessment, and Acting Vice-Chair of IA CoP

Dorotea Manolova, Bulgaria, Co-leader of Working Group on Risk Assessment

Diana Grosu-Axenti, Moldova, former Chair of the IA CoP

Arman Vatyan, World Bank, Coordinator of the IA CoP

The following individuals invested key efforts in establishment and initial operation of the Risk Assessment Working Group:

Joop Vrolijk, OECD/SIGMA

Albana Gjinopulli, Albania, former Leader of Working Group on Risk Assessment

Acronyms

CHU	Central Harmonization Unit
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
EU	European Union
HIA	Head of Internal Audit
IA	Internal Audit
IA CoP	Internal Audit Community of Practice
IIA	Institute of Internal Auditors
IT	Information Technology
PEM-PAL	Public Expenditure Management Peer Assisted Learning
RAP	Risk Assessment in Audit Planning
UN	United Nations
WB	World Bank

Introduction

Background and purpose of the guide

1. The Risk Assessment in Audit Planning (RAP) guide, drafted by the PEM-PAL Internal Audit Community of Practice (IA CoP), emphasises the importance and the impact that an effective audit strategy and audit plan for the achievement of the goals, objectives and the mission of the internal audit unit. Planning provides for a systematic approach to internal audit work and requires knowledge covering a wide range of issues in public management, including risk assessment and internal control.
2. This RAP guide has been developed to:
   - Help Internal Audit units to produce effective risk-based strategic and annual plans.
   - Provide a guidance on planning and risk assessment that can be used as a set of principles by central units responsible for advising on the development on Internal Audit in their own countries.
3. The guide is fully consistent with the Institute of Internal Auditor's (IIA) International Standards for the Professional Practice of Internal Auditing on planning internal audit work. In particular:
   - IIA Standard 2010 which requires "The chief audit executive1 must establish risk-based plans to determine the priorities of the internal audit."
   - IIA Standard 2010.A1 which requires that "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".
   - IIA Standard 2010.A2 "The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions."
   - IIA Standard 2020, "The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations."
4. These standards require the Head of Internal Audit (HIA)[2] to develop a risk-based plan. The HIA should take into account the organisation's risk management framework, including risk appetite levels set by management for the different activities or parts of the organisation. If a risk management framework does not exist, the HIA uses his/her own judgment of risks after consideration of input from senior management and the board. The HIA must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programs, systems, and controls.

1 The chief audit executive is referred to as Head of Internal Audit for the purposes of this document which is a more relevant term for the public sector as agreed by IA CoP.
2 Or an individual appointed to implement this role.

Why is risk-based planning important for an internal audit unit

5. The main challenge faced by majority of internal auditors is how to allocate limited internal audit resources in the most effective way - how to choose the audit subjects to examine. This requires an assessment of risk across all the auditable areas that an auditor might examine.
6. The objective is of risk-based planning is to ensure that the Auditor examines subjects of highest risk to the achievement of the organisation's objectives.
7. Strategic and annual audit plans must be developed through a process that identifies and prioritizes potential audit topics. The entire population of potential auditable areas, which can be categorized in many ways, is called **the audit universe**[3]. For each element of the audit universe the risks or opportunities have to be assessed and decisions taken on other risk factors that may influence the priority to be given to each element of the audit universe (**audit objects**).
8. The strategic and annual plans are important documents, which are normally presented to management. The strategic plan provides an opportunity to present the work of the internal auditor and the benefits that will arise from the audit function. It represents a shop window, which explains what internal audit can do for management. The annual plan translates the strategic plan into the audit assignments to be carried out in the current year. The strategic and annual plans must be clearly structured and well written and should provide management with a persuasive summary of the logic supporting the judgments made on the priority given to certain topics. A structured approach to risk-based planning is an important step towards an effective audit strategy.

How to use the guide

9. The RAP guide is presented in five chapters as follows:

    - Chapter 1 "Understanding risk-based planning" considers the fundamental features of risk-based planning and the conceptual framework used in the guide.
    - Chapter 2 "Categorizing the audit universe for risk-based planning" considers how to categorize the audit universe for risk-based planning.
    - Chapter 3 "Identifying risks and assessing their probability and impact" considers how to identify and assess risks in terms of their probability and impact on the organisation's objectives.
    - Chapter 4 "Building risk-based strategic and annual plans" considers how to use risk factors and scoring criteria to identify audit objects for inclusion in strategic and annual audit plans.
    - Chapter 5 "Writing and updating strategic and annual plans" considers how to develop strategic and annual plans and how to keep them up to date.

10. The guide contains generic guidance and also includes:

    - Examples drawn from generic research on internal audit practice;
    - Example of practices across PEM-PAL countries (collected through a survey); and
    - A number of general hints and tips on key issues – these are the type of support that an experienced auditor would pass on to a less experienced colleague.

General hints and tips are presented in orange boxes.

3 See Chapter 3

Chapter 1. Understanding risk-based audit planning

What are risks?

11. The key definitions concerning risk are:

- Event – an incident or occurrence, from sources internal or external to an organisation, 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 is the possibility that an event will occur and adversely affect the achievement of objectives. Risk is measured in terms of impact and likelihood.
- Opportunity is the possibility that an event will occur and positively affect the achievement of objectives.
- 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 is 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 is 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.)
- Risk appetite is the level of risk that an organisation 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.

Understanding the differences between risk management and risk assessment in audit planning

12. Risks are considered by both managers and auditors and are similarly defined[4].

- Risk management is (or should be) an integral part of internal control system5 and is the responsibility of management. It is a structured process where managers (a) examine likely future events and the risks and opportunities these represent to the achievement of organisation's objectives; and (b) determine and implement risk management actions (e.g. control activities).
- Audit risk assessment is part of planning and a process where auditors consider both (i) individual events and the risks and opportunities these represent to the achievement of the objectives of elements of the audit universe and (ii) generic

4 Note: auditors must also consider "Audit Risk" which is a specific risk that arises because of the selective nature of audit work - the possibility that the results of an audit are not correct.

5 See the guidance in internal control produced by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) for more information on the link between risk management and internal control.

risk factors that help prioritize work to areas of highest risk. The purpose of audit risk assessment is to ensure that scare audit resources are addressed to the audit of areas of highest risk to the organisation.

☑ **No one can assess risk, if objectives are not clear**. If it is not clear what an element of the audit universe is trying to achieve you cannot carry out a risk assessment. Be sure you understand the objectives of different elements of the audit universe before trying to identify likely events that impact these objectives and the inherent and residual risks involved.

The auditing standards state clearly that where management has a functioning risk management system in place auditors should use this as a basis for carrying out their own risk assessment.

13. While risk management is a logical process, many public sector organisations do not address risk management in a consistent and structured way and do not have effective internal control. In this situation auditors must make their own judgements about risk within the organisation. In other words: *the auditor must assess risks to the achievement of the organisation's objectives even if management do not*.

☑ If a strong risk management process exists this can be reviewed by internal audit (IA) as part of their annual planning process.

☑ Even where IA has to carry out their own risk assessment they seek management input on such things as the organisation's appetite for risk.

☑ An IA of risk management processes conducted to encourage better risk management in the organisation, can often be a very productive audit for an internal auditor.

A conceptual framework for risk-based audit planning

14. To develop a risk-based plan the auditor needs to consider two aspects of risk:

    (a) individual events/risks and how these may impact the achievement of the organisation's objectives (see Chapter 3); and

    (b) generic risk factors that may suggest a higher or lower level of risk and which can be used to determine the priority that should be given to a single audit within the audit universe.

15. Where an organisation has already put in place risk management processes the auditor can examine risk registers to see what individual risks have been identified by management and the action being taken to address these. Where there is no risk management process in place the auditor will need to identify possible events that may generate risks and assess these in terms of impact and probability.

16. The basic conceptual framework for risk-based audit planning therefore has five distinct stages:

    1. Determining and categorising the audit universe. (See Chapter 2)
    2. Identifying individual events that may give rise to risks and opportunities across the audit universe. (See Chapter 3)
    3. Scoring events in terms of probability and impact (taking into account management actions to mitigate risk) to identify the level of residual risk. (See Chapter 3)

4. Building risk-based audit plans by using generic risk factors and scoring criteria for each factor to determine the audit priority of all audit objects within the audit universe. (See Chapter 4)
5. Presenting the results of risk-based planning by writing and updating strategic and annual work plans. (See Chapter 5)

Taking into account Entity Risk Management processes

17. The planning process must consider the extent to which management have already assessed risk and what common elements of this assessment the auditor can use. Table 1 below compares the common elements of risk management with a typical risk assessment process in audit planning.

Table 1 The common elements of risk management and risk-based audit planning

Risk management stages	Risk-based audit planning stages
Objectives should be set by management before undertaking a risk assessment.	
1. Identifying events that may give rise to risks and opportunities to the achievement of objectives.	1. Determining and categorising the audit universe.
2. Scoring events in terms of probability and impact to identify the level of **inherent** risk.	2. Identifying events that may give rise to risks and opportunities across the audit universe. *This is essentially the same process but is related to the audit universe.*
	*The auditor will be very interested to know how management have assessed **inherent** risk but the main concern for planning purposes is **residual** risk. So this review must take into account steps 3 and 4 of risk management.*
	Auditors are not responsible for determining the risk response but may have views on its effectiveness. (For example, managers may consider it is not necessary to control a particular risk whereas the auditor may think it would be better to do so.)
	*Auditors are not responsible for putting in place mitigation actions and must assess the effectiveness of control activities in terms of its impact on **residual** risk.*
3. Determining an appropriate risk response (whether to accept the risk, to avoid the risk, to transfer the risk to others, or control the risk).	3. Scoring events in terms of probability and impact (taking into account management actions to mitigate risk) to identify the level of **residual** risk.

Risk management stages	Risk-based audit planning stages
4. Putting in place the risk mitigation action decided upon to arrive at an acceptable level of residual risk – this includes control activities.	4. Developing generic risk factors and criteria for each factor to identify the audit priority of audit objects within the audit universe.
	5. Developing and maintaining risk-based audit plans (strategic plan and annual work plan).

From the table it is clear that there is a significant overlap between the first two stages of risk management and the second and third stages of audit planning risk assessment.

19. The main difference is that managers need to assess ***inherent*** risks so that they can determine and put in place risk mitigation actions (including controls). The auditor however needs to assess ***residual*** risk (which is the risk that remains after the effectiveness of internal controls are taken into account) to determine areas that are high priority for examination.

20. A simple example illustrates the relationship between inherent risk control activities and residual risk: *If you cross the street, there are a nearly infinite number of inherent risks. One of the inherent risks with a high probability and large impact would be getting hit by a car. So to mitigate this risk we implement the control of looking left and right to check for oncoming traffic before crossing the road. But this will not eliminate every possible risk and residual risks remain. For example, you could still be hit by a meteor because you did not look up!*

21. The reason for this is obvious. With limited resources the auditor wants to concentrate audit work on areas where the risk exposure to the organisation is highest. If inherent risk is very high but there are good controls in place then the residual risk may be low and not therefore worthy of examination.

☑ ***Understand the difference between inherent and residual risk:***
Inherent risk – control activities = residual risk.
The auditor's focus in risk-based planning is on identifying high levels of residual risk.
Where an organisation is new and/or there is no information about the effectiveness of control activities the situation is that:
Inherent risk = residual risk

The actions required to implement risk-based planning

22. The table below shows the key actions required to implement the conceptual framework for risk-based planning and how this would differ for organisations with or without risk management systems in place.

Risk-based audit planning stages	Risk management in place	No risk management in place
1. Determining and categorising the audit universe. ***(See Chapter 2)***	✓ *Identify categories for splitting the audit universe into discrete auditable objects.* ✓ *Discuss and agree approach to categorisation with management.* ✓ *Identify and list all the audit objects in your audit universe by agreed category.*	
2. Identifying events that may give rise to risks and opportunities across the audit universe. ***(See Chapter 3)***	✓ *Review risk registers to understand the events that managers have identified.* ✓ *Consider completeness of events identified and discuss with managers their views on the organisation's risk appetite.*	✓ *Identifying events that may give rise to risks and opportunities across the audit universe.* ✓ *Discuss risks and opportunities with managers to obtain views on completeness and discuss with managers their views on the organisation's risk appetite.*
3. Scoring events in terms of probability and impact (taking into account management actions to mitigate risk) to identify the level of residual risk. (See Chapter 3)	✓ *Review the way that management have scored events and the actions put in place to address key risks.* ✓ *Consider effectiveness of risk mitigation actions in terms of its impact on residual risks.* ✓ *Identify high levels of residual risk that need to be factored into strategic and annual work plans.*	✓ *Score events in terms of probability and impact (taking into account management actions to mitigate risk) to identify the level of residual risk.* ✓ *Discuss approach with managers and obtain agreement on the way risks are being scored.*
4. Developing generic risk factors and criteria for each factor to identify the audit priority of audit objects within the audit universe. ***(See Chapter 4)***	✓ *Produce initial list of risk factors.* ✓ *Determine criteria for scoring each risk factor.* ✓ *Decide whether to add a weighting to each risk factor.* ✓ *Discuss the approach with management and obtain their views on the relevance of the risk factors chosen, the criteria to be used in scoring and the weighting to be given.* ✓ *Score each risk factor to identify high medium and low priorities for all audit objects in the audit universe.*	

Risk-based audit planning stages	Risk management in place	No risk management in place
5. Developing and maintaining risk-based audit plans (strategic plan and annual work plan). ***(See Chapter 5)***	✓ *Determine the strategy and cycles of coverage for different categories of the audit universe based on the risk factor scores.* ✓ *Develop a strategy document that supports the choices made and explains the methodology used and judgements made to arrive at decisions.* ✓ *Develop an annual work plan in line with the strategy identified the specific audits to be undertaken, their titles, timing and expected duration.*	

Chapter 2. Categorising the audit universe for risk-based planning

What is the "audit universe"?

23. The IA CoP's Good Practice Internal Audit Manual template explains that the audit universe is the "*starting point for the internal audit plan"* and defines the audit universe as: *"The overall scope of the internal audit function and the totality of auditable processes, functions and locations".*

    - The phrase "audit universe" is a simple way of referring to all the totality of all things that an internal auditor could separately examine.
    - The universe consists of the totality of "auditable objects" which is a way of identifying and describing discrete part of the business, system or process, which can be separately audited. Auditable objects need to be large enough to justify an audit and small enough to be manageable.

The elephant approach - cutting the audit universe down into small chunks

24. The answer to the question: "*How to eat an elephant?"* is "*One bite at a time".* This is the way we need to treat the audit universe by cutting it into specific systems, processes, programmes or organisational units that can be audited – ***auditable objects***.

25. Traditionally, auditable objects were categorised by organisational structure and were defined from the top down - a "***vertical"*** analysis. Often an auditable object equated with one or a number of organisational units. This remains a useful first cut of the audit universe that most IA units use.

26. However, this may not be the most effective way to plan all possible audits. It is therefore also important to design audit coverage from a ***horizontal*** or ***cross-functional*** view of the organisation - that is 'horizontal' audits based on entire business processes. For example, an organisation's accounting or business management systems can be said to operate horizontally because that affect all organisational units. These systems may pose critical risks across several processes and should therefore be examined horizontally.

27. Typically therefore the audit universe is a mix of a number of top down (vertical) and cross-functional (horizontal) slices. Procurement is often a key cross-functional activity. However it could be split for audit purposes into location and type of purchase. In the UN World Food Programme, for example, procurement could be split into four audit objects: headquarters procurement, local office procurement, procurement of food, and procurement of non-food items. This would be appropriate because each element has different rules regulations and internal controls.

28. There is a high degree of commonality in the way that IA units in Government typically cut up or categorize the audit universe (see good practice examples below and Annex C for example of PEM-PAL countries).

Table 2 Good practice example on categorisation of the audit universe

From IIA Government survey
1. Almost all IA units have a formally documented audit universe (97%)
2. The most common categorisations used are:
• Departments – 97%
• Processes – 97%
• Organisational unit or location 81%
• Operational programmes – 75%
• Service Lines – 58%
• ERM risk portfolio – 28%
• Other – 22%

29. Ultimately it is for the HIA 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 (Departments, Divisions, Units, Stand-alone Projects);
    - By common processes (Payments, Receipts, Asset Management, Procurement, Contracting, Inventory, Human Resource Management);
    - By location (Headquarters, Regional offices, Local offices);
    - By operational programmes (e.g., in a transport agency or department these could include: construction of new roads, maintenance of roads, issue of licences for drivers, collection of speeding fines, etc.);
    - By service lines (e.g., in a social security department these could include: services for the elderly, services for the handicapped, services for the care of children which may be handled by a number of different departments or units).

Example - Internal audit of the UN Food and Agriculture Organisation

The audit universe of the office consists of some 100 auditable entities that are divided into 14 categories: 1) Governance, 2) Reforms, 3) Strategic Management, 4) Special Initiatives/Projects, 5) Planning and Budgeting, 6) Field Programme Cycle, 7) Decentralized offices, 8) Information Systems and Technology, 9) Knowledge and communication, 10) Safety and Security, 11) Human Resources, 12) Financial Management, 13) Procurement, Property and Facilities management, and 14) Administrative and Other Services.

☑ ***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.*

☑ *The categorization of the audit universe is something that takes a lot of thought and may change as the planning process evolves and you consider individual risks and opportunities (Stage 2, as per paragraph 17).*

Remember that you will present the categories in your audit strategy so they should make sense to the managers of the organisation.

Seek senior managers' opinions

30. Senior managers must be consulted for their views on the importance of the systems identified, and the existing controls and general control environment. Discussions with these managers should be conducted in an open manner and focus on:

- Clarifying the organisation's main objectives and the role of individual departments in achieving these;
- Identifying the main risks they face in achieving the organisation's and their departmental objectives;
- The results of internal and external audit work carried out during the year;
- Any areas of concern that the managers may have over internal control or efficiency within their department or the organisation's priorities for assurance and audit attention.

Chapter 3. Identifying risks and assessing their impact and probability

31. Having identified the audit universe of auditable objects the next step in the process is to identify specific risks. The objective is for IA to obtain a thorough understanding of the risks facing the organisation and their potential impact and probability, so that this knowledge can be used when scoring generic risk factors to select audit objects for examination (as explained in Chapter 4).

☑ ***Risk is a general term that can be difficult to grasp****. However, almost everyone understands what an event is. Thinking of events that could impact objectives is the easiest route to identifying risks.*

☑ ***Links between categorising the audit universe and identifying risks.***

- ✓ *Identifying major risks may suggest changes to the way that the audit universe is categorised. For this reason identifying risks and categorising the audit universe may be carried out at the same time or in an interactive way.*
- ✓ *The categories used for the audit universe can also be useful in brainstorming possible events.*

Good practice is that risk identification and risk assessment (scoring for impact and probability) should be carried out in two phases. The reason is that the first phase (risk identification) is very similar to "brainstorming" where the objective is to capture all risks. The second phase is about applying realistic judgements on the importance and probability of risks identified. It can be complicated to combine these two different ways of thinking about risk.

☑ ***Carry out risk assessment in two clear phases****. Use phase one to identify risks and phase two to assess (score) risks in terms of impact and probability.*

Identifying events that may give rise to risks and opportunities across the audit universe

32. The approach to identifying events will be different if management already has an entity risk management process which identifies events and assesses risks.

- Where a risk management process is in place IA will need to (a) examine risk registers to understand the events that managers have identified and then review these to determine whether the risk assessment has identified all the key risks; (b) review the way that management have scored events and the actions put in place to address key risks; (c) consider the effectiveness of risk mitigation actions in terms of its impact on residual risks; and (d) identify high levels of residual risk that need to be factored into strategic and annual work plans.
- Where no risk management process is in place IA will need to carry out a separate exercise to identify events that give rise to risks and opportunities. This is more difficult and time consuming than reviewing management's own risk assessments.

It is important that the process includes interaction with management to obtain their views on key events and risks impacting the organisation. It will also be necessary to score events identified in terms of probability and impact to create an overall risk score.

33. The process of identifying events and scoring risks as part of a separate exercise is considered in more detail in the sections that follow.

Identifying risks

34. Even where management has not carried out formal risk assessments there will often be other documentary sources that can help IA unit to identify individual risks. These include:

- Operational plans for the organisation;
- Earlier reports by internal or external audit;
- Annual report of the organisation;
- Major reviews of functions or activities carried out by management or by external bodies (e.g. WB or EU review missions).

35. The most common method of identifying risks will be by interview and discussions with management. This should always be done, as management's views on risk are very important.

☑ ***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.*

- ✓ *The first part of the workshop would be devoted to identifying risks;*
- ✓ *The second part of the workshop would assess (score) identified risks for impact and probability.*

To identify risks it can be useful to brainstorm the different types of events that may generate risks for the organisation. An example is provided below of common types of events that generate risk.

Examples of types of events that may generate risks					
Operational	**IT & communication**	**Regulatory**	**Financial**	**Personnel**	**Reputation**
Loss or inaccessibility offices Unavailability of staff Utility failures (electricity, gas, or water) No transportation Critical equipment/ hardware failures Loss of supplies and materials	Loss of internet Loss of telephones Data unavailable or destroyed Data corrupted Viral attacks on key software Hardware failures Vital records destroyed or canned be accessed	Contract violations Non-compliance with key legislation EU fines for non-compliance with regulations	Budget cuts Loss of grant or funding Theft or misuse of funds Lack of cash for operations	Loss of key staff (resignation, retirement) Accidents involving staff Lack of integrity of managers Lack of skills and qualifications	Negative media publicity Levels of service below expectation Loss of trust from stakeholders because of operational shortcomings

Assessing risks in terms of impact and probability

36. Once all relevant events (risks) have been identified they need to be assessed and scored. Inherent risk should be assessed in terms of **impact and probability**. The impact defines the financial or non-financial consequences for the organisation should the risk occur. The probability defines the chances that the risk may occur. Assessing impact of risks is more complex than assessing probability but both are important elements of a risk assessment.

37. It is recommended not to score the risks in a pure mathematical way. It is more practical to assess and score them according to predetermined criteria for impact and probability. Good practice often suggests using three scoring levels, but this may lead to an over-scoring in the middle category. A four point scales may therefore be the most appropriate (particularly for assessing impact). There is no defined rule here. Auditors are free to choose whichever scoring system they feel is more appropriate. The example below uses four categories and three could also be used.

Criteria for assessing impact

38. There could be many criteria for assessing risk impact but those limited to four or five considered to be the most important. The following **criteria for assessing impact** are commonly used and should be considered:
    - Financial impact. The monetary consequences for the organisation should the risk occur.
    - Impact on reputation. The consequences with regard to the reputation of the organisation, minister or even at a higher level the reputation of the entire country in the eyes of rating agencies, international development partners, 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/achievement of objectives/operations. The extent to which the mission of the organisation may be impacted by the occurrence of the risk.
    - Impact on people. Unplanned loss of key people and skills can significantly impact organisation.
39. For each risk impact criteria the auditor needs to define what would represent different levels of impact (Very High, High, Medium, and Low). This will ensure that risks are scored in a common way. The example below provides general advice on scoring three criteria.

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 Organisation. 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 Organisation. Slow systems recovery.
Very High (4)	Significant material financial impact that is more than xxx,xxx.	Serious injury/death to personnel.	Organisational wide inability to continue normal business. Significant loss of operations. Widespread service interruption. Slow systems recovery.

Annex A provides an example of risk impact criteria used an IA unit in a UN Agency.

Criteria for assessing probability

40. The auditor needs to consider the probability of an event occurring. For example, an earthquake could have a very high impact but they not occur very often. The impact of loss of people or skills may not be very high but it may occur very often. The criteria for assessing probability are often very similar and the following could be considered as an option.

Level	Criteria	Score
Rare	Event extremely unlikely to happen	1
Unlikely	Event has a remote possibility of occurrence	2
Medium	Event fairly likely to happen sometime in the future	3
Likely	Event will likely occur (within 1-2 years)	4
Expected	Event is already occurring or expected to occur	5

Scoring risks for impact and probability

41. Having developed criteria for assessing (scoring) impact and probability these need to be applied to all the risk identified. This can be done in different ways:
    - Score sheets can be developed and used by individuals to assess risks and then the results of individual scores combined to develop an average across a group of people.
    - Scoring can be done in a meeting where each individual presents his or her view and a consensus score is agreed.
42. Whichever method is used remember that people assess risks in different ways. Some people are by nature risk averse and others are risk takers. If one person assesses a risk as high and the other as low, the result should not simply be medium. A consensus needs to be reached.

Combining assessment criteria into a risk matrix

43. Decisions will need to be taken on combining the scores for risk impact with risk probability. Many organisations use a matrix and agree in advance which combinations of probability and impact represent low, medium, high and very high risk.
44. An example of a typical matrix is shown below. This would need to be modified to reflect the actual method of scoring impact and probability. Different decision can also be taken on which combinations to classify as low medium or high.

Rare/ Improbable Unlikely 1 2			PROBABILITY				
			Medium	Likely	Frequent/ Expected		
			3	4	5		
IM-PACT	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

☑ ***Remember the goal of this stage of the process is to obtain a good understanding of risks in the organisation.***

- ✓ *Internal audit should only be assessing individual risks if management is not doing this already.*
- ✓ *Internal audit should encourage management to develop effective entity risk management processes as part of internal control.*

Chapter 4. Building risk-based strategic and annual plans

45. By this stage the auditor should have a good understanding of risks that may impact the organisation. But how important are these risks in relation to different elements of the audit universe? And how these risks can be reflected in the audit strategy and annual work plan?

46. The objective of this stage of the process is to determine what needs to be audited from within the audit universe. To identify the building blocks for the audit strategy in terms of the types and cycles of audits that need to be undertaken. This is why this process is also referred to as an "*audit needs assessment*".

47. Because 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. While the term *risk factors* is used these could also be described as *selection factors,* because the purpose of this stage of the process is to select the most appropriate audits to undertake.

☑ ***It may be helpful to think of "risk factors" as "selection factors"*** *as the goal of the process is to select which audit objects should be audited and how often this should be done.*

Identifying risk factors

48. Most organisations use between five and eight risk factors. With less than five on average for government internal auditors. All IA units surveyed by IIA use *degree of financial materiality* as one of the risk factors (Table 3).

49. The most commonly used risk factors, with explanatory comments as to why they are important, are:

Financial materiality. The volume of financial activity covered by an auditable object is a key risk factor. High-risk audit objects that use a very small part of the budget may be of less priority for audit than medium risk audit objects that deal with 50% of the budget.

Complexity of activities. Complex activities are more difficult to do well and therefore more likely to not achieve their objectives e.g. construction projects often cost more than planned and take longer to complete than expected.

Control environment (as defined in COSO). The control environment is sometimes referred to as the "tone at the top". A strong control environment is less susceptible to fraud and error. In a strong control environment there are: clear objectives, organisational roles & responsibilities, clear ethical standards of behaviour, strong governance arrangements, and effective people management policies and practices. A weak control environment is more susceptible to fraud an error.

Reputational sensitivity. Some areas will have a higher media profile where problems can generate a high level of risk to the reputation of the organisation as a whole.

Inherent risk. Areas of high inherent risk will require effective control processes to reduce the risk involved. Such important controls should be reviewed more regularly by IA.

Extent of change. Change is known to generate increased risk. For example: high turnover of staff is likely to reduce the effectiveness of controls as staff are less experience; reorganisation of functions or change of leadership/key managers can also generate uncertainty for staff which limits their effectiveness.

Confidence in management. Good managers usually solve problems more efficiently and achieve better results than poor managers and more experienced managers are more likely to be able to identify and deal with risks. Remote units that are managed by lower grade staff may be of higher risk.

Fraud potential. Some systems and functions are more prone to fraud and corruption. For example, high levels of cash receipts and delegated responsibility to impose fines.

Political sensitivity. Some subjects are may be more political sensitive than others and therefore of attract higher interest from stake-holders.

Time since last audit. There is a deterrence factor in every audit. Even auditable objects with low risk should be audited from time to time. And those which have not been audited for a number of years may become high risk.

☑ ***Note that inherent risk can be a generic risk factor.*** *The work done under Chapter 3 to identify and score risks can be used to identify areas of high inherent risk.*

Table 3 Good Practice example - common risk factors used by IA units

From IIA Government survey
The most common categorisations used are:
• Degree of financial materiality - 100%
• Complexity of activities - 94%
• Control environment - 94%
• Reputational sensitivity – 92%
• Inherent risk – 92%
• Extent of change – 89%
• Confidence in management – 83%
• Fraud Potential – 81%
• Time since last audit– 78%
• Volume of Transactions – 78%
• Degree of automation – 72%

See Annex C for example of PEM-PAL countries.

50. The decision on which risk factors to use is important and should include at least some of the main risk factors used in general by internal auditors.

☑ ***Keep the number of risk factors to between 4 and 8.*** *Too few risk factors will limit the effectiveness of the exercise, too many will increase the time it takes to and will not produce substantially better results. Remember you have to develop criteria to assess each factor and score them.*

☑ ***Choose risk factors that make the most sense for the organisation you are auditing.*** *Don't only use the list above if there are other factors that are more relevant.*

Develop criteria to assess the importance of each risk factor

51. Having identified a number of risk factors it is common practice to develop a set of criteria than can be used to score and therefore rank the relative need to audit each of the possible audit objects within the audit universe. Developing criteria can be relatively simple or quite complex. But many factors will use some degree of judgement so it may be easier to define only the lowest or highest score and leave the rest to judgement. The example below provides possible criteria for four common risk factors three of which are judgemental in nature (control environment/vulnerability, sensitivity and management concerns).

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 system 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 organisation 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

Consider adding a weighting to each risk factor to produce a risk index

52. Not all risk factors will be equally important. Many IA units therefore use some process of weighting risk factors to give a higher score to those factors considered most important (for example materiality or management concerns). Having added a weighting factor, which could be developed in a workshop with management, the score for risk factors and weighting score need to be multiplied to produce a numeric risk index. The risk index can then be used to identify audit objects with very high, high, medium and low priority. The following example shows how this would apply in the example shown for risk factors.

Example of weighting risk factors

Step 1 Each of the risk factors is given a weighting using judgement of the relative importance 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.

All risk-scoring systems by definition produce exact numbers. This can add a false level of accuracy to the assessment process. It is important to recognise that many risk factors are judgemental and are not based on absolute values. A major exception is materiality, which is also one factor that will usually be highly weighted. (Note: There are many ways of determining materiality but the simplest models usually use a percentage of total expenditure or income.)

☑ ***Make sure that risk index scores and priorities are reasonable.*** *(a) Calculate the theoretical maximum before setting the index priorities and (b) be prepared to change the index priorities if the results are obviously unrealistic (for example if every audit is show as high priority).*

Chapter 5. Writing and updating strategic and annual plans

53. A comprehensive strategic and annual plan of IA activity is crucial to the success of internal audit. Having identified and assessed risks across the audit universe the next step in the process is to develop plans to address the areas of highest importance. Planning ensures a systematic approach to IA activities and requires knowledge and competence in a wide range of areas, such as risk assessment and internal control

Strategic plan

54. The purpose of the strategic plan is to document the judgements made about "audit needs" – the internal auditor's judgement of the systems, activities and programmes that should be subject to audit to provide reasonable assurance to management about risks and the effectiveness of internal control. The plan must contain:

- Clearly expressed objectives and performance indicators for what the IA function will achieve in the next 2-4 years, linked as appropriate to the strategy for the organisation.
- The methodology used to prepare the strategy and how the IA unit has assessed risks that impact the organisation's objectives.
- How the IA unit will address the areas of most significance over a period of years. It will usually be necessary to identify cycles of coverage for different elements of the audit universe. Some systems and processes may need to be examined every year. Others may only need to be examined every three to five years and so on.
- The resources required and available to meet these needs and the impact of resource constraints on the ideal level of audit coverage.
- An internal risk assessment of those events which may impact the achievement of objectives in the audit strategy and mitigating actions to address such risks. (For example, staffing shortfalls; skills shortages and training and other actions needed to address these risks.).
- Plans for the coordination of work with other sources of assurance (e.g. external audit).
- The approach for following up recommendations made.
- The higher or longer-term goals the IA function wants to achieve but may not achieve in the short term.

A strategic plan is a "shop window" for internal audit – use it well. *The strategy is an opportunity to present to management all the things that an IA unit could do to help the organisation achieve its objectives. It can be useful way of generating support.*

Annual audit plan

55. The annual audit plan translates the strategic plan into the audit assignments to be carried out in the current year. It should define the purpose (title and objectives) and duration of each audit assignment and allocate staff and other resources accordingly. The plan should provide a basis for agreeing the assignments to be undertaken and the timing of each assignment with the relevant managers. As these need to be geared to the budgetary resources available it is usually preferable for the audit plan to mirror the budgetary period.

56. In developing the annual plan, the HIA should consider several inputs in order to get a realistic work plan that provides added value to the organisation:

- The strategic audit plan assumptions and whether these are still valid in the light of audit findings.
- The latest annual plan (if appropriate), taking consideration the main findings from previous audits that indicating changes in risk.
- Organisational and timing constraints. (For example: changes in departmental Organisation; locations that cannot be reached in the winter months; major periods of leave or office closure – Christmas, Easter, Summer, implementation of new IT systems; high workload periods.)
- The resources that should be reserved for future unplanned work (see below) to avoid frequent reshuffling of the annual plan.
- Optional program of audits to take the place of postponed audit missions and/or a lower volume of unplanned work than forecasted.

57. Plans should be prepared before the year begins. Not all audits will be completed within a planning year so the plan for the coming year must take into account work that crosses the year-end.

☑ ***Plan for the resources actually available.*** *While empty posts may be filled during the year it is advisable to plan for the resources you know you have, not the resources you think you may have.*

☑ Allow sufficient time for planning and reporting the audit work completed.

☑ ***Nothing ever runs to plan****. Make some assumptions about slippage – allow sufficient time for management responses to recommendations.*

Keeping plans up to date – regular monitoring of risk

58. Risk is not a static concept. It changes over time. In addition, events that actually happen (e.g. a major reduction on budget) will generate new risks for the organisation. (For example, the achievement of a major capital project, which was low risk when funds were available, may be high risk because of a budget revision.)

59. Auditors must therefore monitor significant events that occur during the year (e.g. by reviewing new official documents, external reports, media coverage and change in the legal framework) and the impact these may have on the audit plan. (For example, a change of minister with very different views on the highest priority projects in the budget.)

Annual review of the strategic plan

60. Planning is a dynamic process. New systems, more up-to-date information and other developments affecting the organisation may result in a reconsideration of audit needs assessment. For this reason both the audit risk assessment and the strategic audit plan should be reviewed annually. The plan should be completely reassessed towards the end of the cycle.

61. In reviewing the strategic audit plan, the HIA should consider:
    - Changes that have occurred to the organisation, its activities, objectives or its environment. This may effect the risks that it faces in achieving its objectives and consequently the relative risk of each auditable system.
    - Results of IA assignments undertaken in the previous year may lead to the original assessment of risk and priority being revised. These may indicate the need for a redirection of audit effort, for example, by revisiting a particular system or by examining a related system.
    - Whether budgets are still appropriate and will ensure the delivery of an efficient IA service.

☑ ***Update Risk assessment each year***
It will normally be necessary to update the formal risk assessment each year and to revisit the scoring of risk factors to see whether the priority of audit objects has changed during the year.

☑ ***Consider significant events arising during the year***
If there has been a significant event during the year which has a major impact on risk (e.g. a major cut in budgets) it may be necessary to review the risk assessment and selection criteria immediately to determine whether the annual work plan needs to be changed.

Dealing with additional requests for audits during the year

62. No plan is perfect. Changes are inevitable and may arise for many reasons:
    - The organisation may be reorganized;
    - New senior managers may have different views on the priority to be given to particular activities;
    - A major fraud may be detected identifying higher levels of risk in a particular area;
    - The Minister may request an earlier review of subjects planned for later in the strategy.

63. The HIA also need to maintain a balance between responding positively to such requests and the need for the overall programme of work to provide an adequate level of assurance in relation to the main risks identified. For each request for ad hoc work there should be a discussion with senior managers of the benefits of responding to the request and the impact this will have on the annual work plan. The results of this discussion should be documented.

64. Where the HIA agrees to undertake an assignment not included in the annual work plan the remainder of the work should be reprogrammed and a revised work plan submitted to managers. As a general rule the annual plan should not be updated more than once a quarter.

65. Many IA units reserve a proportion of their resources for handing unplanned or ad hoc work. This is something that HIA should consider over time as they gain experience of the likely level of unplanned work.

☑ Inform managers of the impact of undertaking additional audits during the year. Explain clearly what you will not do if you take on a new assignment.

Annex A. Example of risk assessment criteria for impact

Risk Assessment: Criteria for Risk Impact (example from IA unit of FAO)

Level (score)	Criteria				
	Achievement of objectives	Financial	Reputation (integrity, accountability)	Personnel	Operations
Low (1)	Failure to deliver one Organisational result.	Financial impact that may reduce cash flow by less than USD 500,000.	Incompetence/ maladministration or other event that will undermine public trust at a local level. Short recovery period. Serious irregularity.	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)	Failure to deliver several Organisational results.	Material financial impact that may reduce cash flow by more than USD 500,000 but less than USD10 million.	Incompetence/ maladministration or other event that will undermine public trust at a regional level or a key relationship. Short/Moderate recovery period. Small-scale fraud or corruption.	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 Organisation. Promptly recoverable service interruption.
High (3)	Failure to deliver one strategic objective.	Material financial impact that may reduce cash flow by more than USD10 million but less than USD50 million.	Incompetence/ maladministration or other event that will undermine public trust at an international/ regional level or a key relationship. Moderate/Long recovery period. Large-scale fraud and corruption.	Unplanned loss of several key personnel which 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 Organisation. Slow systems recovery.

Level (score)	Criteria				
	Achievement of objectives	**Financial**	**Reputation (integrity, accountability)**	**Personnel**	**Operations**
Very High (4)	Failure to deliver more than one strategic objectives.	Significant material financial impact that may reduce cash flow by more than USD 50 million.	Incompetence/ maladministration or other event that will destroy public trust at an international level or a key relationship. Long recovery period. Fraud, corruption and serious irregularity at Senior Management level.	Serious injury/death to personnel.	Organisational wide inability to continue normal business. Significant loss of operations. Widespread service interruption. Slow systems recovery.

Risk Assessment: Criteria for Risk Probability (example from IA unit of FAO)

Level	Criteria	Score
Rare	Event extremely unlikely to happen	1
Unlikely	Event has a remote possibility of occurrence	2
Medium	Event fairly likely to happen sometime in the future	3
Likely	Event will likely occur (within 1-2 years)	4
Expected	Event is already occurring or expected to occur	5

Annex B. Example of scoring risk factors

66. The following example of a risk assessment methodology for use in planning IA work is based on the United Kingdom Government Internal Audit Manual.

67. The four risk factors used are:

A Materiality (including both absolute levels of materiality and the amounts of funds passing through a system)

B Control Environment/vulnerability

C Sensitivity

D Management concerns

68. Each of the risk factors is awarded a points rating on a scale of 1-5. The table below explains how these ratings might be applied.

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 system 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 organisation 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

69. Each of the risk factors is also given weighting using judgement of the relative significance of each of the factors. This will vary between different types of organisation.

70. An example of weights that may be applied:

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

The factor score and weightings are then combined into a formula which can be used to calculate the risk index. For example:

$$\text{Risk index} = (A \times 3) + (B \times 2) + (C \times 2) + (D \times 4)$$

71. The formula is then applied to each system to produce a risk index for each system. Each system is then categorised as High, Medium or Low risk-based on the following matrix:

Risk Index	**Risk Category**
Over 49	High
30–49	Medium
Less than 30	Low

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

72. All risk-scoring systems by definition produce exact numbers. This can add a spurious air of accuracy to the assessment process. It is important however to bear in mind that many risk factors are judgemental and are not based on absolute values. A major exception is materiality, which is one factor that should always be highly weighted.

Annex C. Example of IA CoP Countries

The survey was organized on the initiative of the IA CoP and was designed to collect of compatible information from all countries represented in IA CoP for Risk Assessment Working Group.

Representatives of 15 countries filled in the questionnaire as follows: **Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Georgia, Hungary, Kyrgyz Republic, Macedonia, Moldova, Montenegro, Romania, Russia, Serbia and Ukraine.**

1. *Does your country have risk assessment methodology for Internal Audit (IA)?*

Options:

a. No

b. Yes, it is part of internal audit manual which was published by

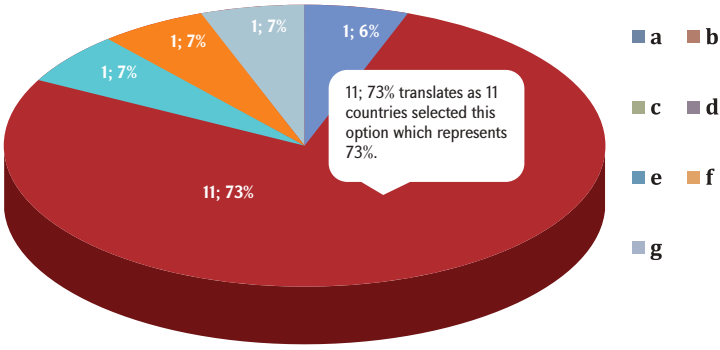
c. Yes, it was published by CHU

d. Not yet, but we are planning it

e. It is under development

f. Each organisation may develop its own RA

g. Other



- In case of 11 countries it is part of IA Manual which was published by CHU.
- In Ukraine each organisation may develop its own RA methodology.
- Georgia has Risk Management Manual which was developed by CHU and adopted by government. They are working on IA Manual and RA methodology will be part of that.
- In Kyrgyz Republic it is under development.

2. *If your country has a risk assessment methodology for IA is it mandatory?*

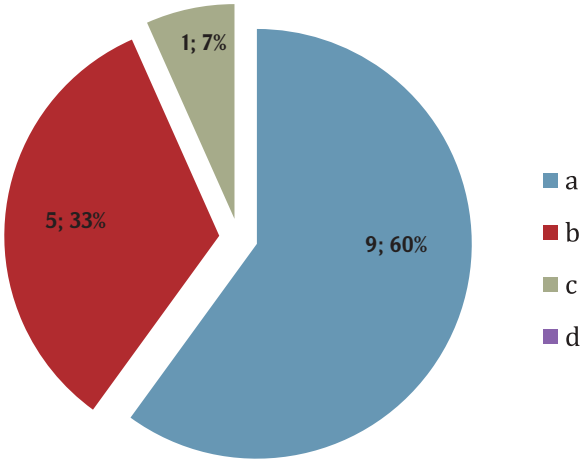
Options:

a. Yes, every entity must follow the methodology

b. No, it is only guidance and it should be adapted to the given entity

c. No, but if IA units have a different methodology it should be approved by CHU

d. Other

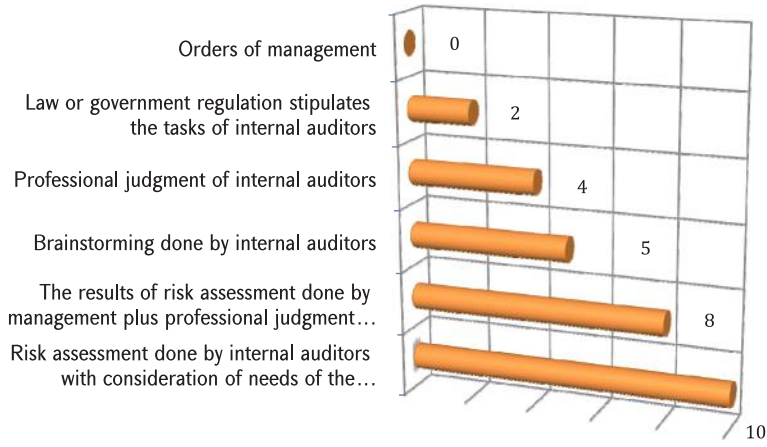


- In 9 countries it is mandatory.
- In 5 countries it is only guidance and it should be adapted to the given entity.
- In case 1 country it is not mandatory, but if an IA unit have a different methodology it should be approved by CHU.

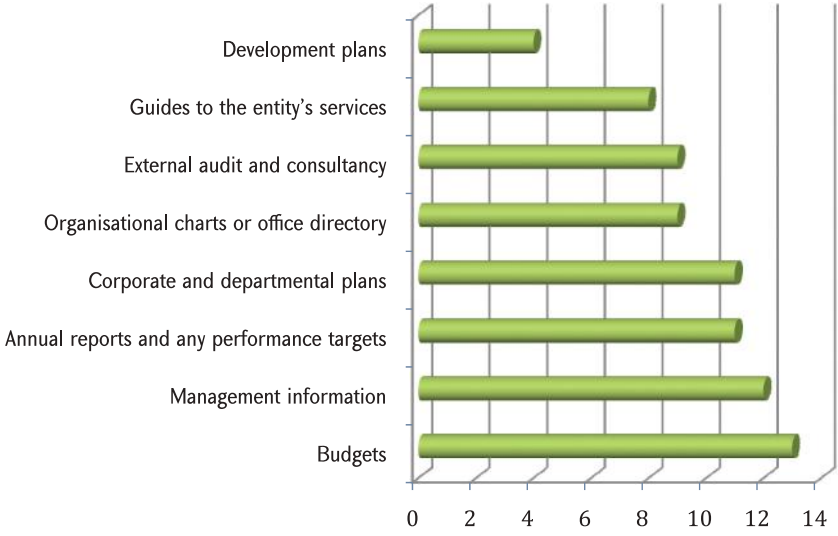
3. *In your country what is the basis of strategic planning by IA?*

Please see responses to question 4.

4. *In your country what is the basis of annual planning[6]?*

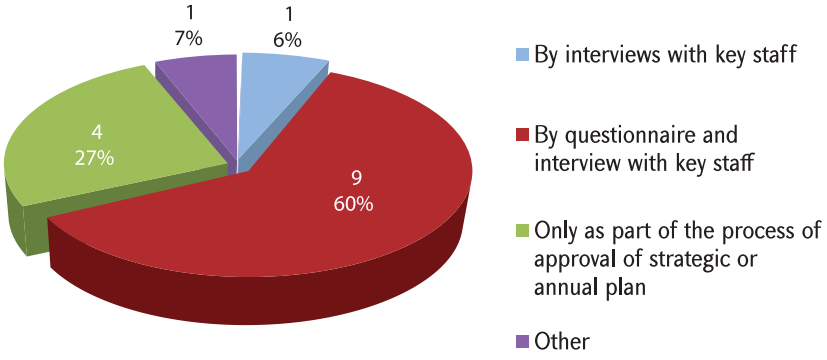


5. *What information sources are used for categorizing the audit universe?*

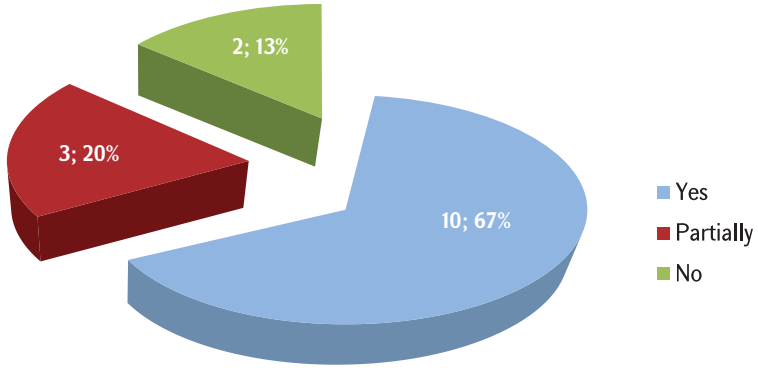


6 Full texts of the last two questions are:
- The results of risk assessment done by management plus professional judgment of internal auditors
- Risk assessment done by internal auditors with consideration of needs of the management

6. How do IA units involve the senior managers of the organization in planning?



7. Do all IA units have (or should they have) a formally documented audit universe?



8. What categorization of the audit universe is used in your country?

Options:

a. By departments
b. By processes
c. By organisational unit or location
d. By operational programmes
e. By service lines
f. By risk management portfolio
g. Other

Answers:

- 7 countries use the categorisation by processes, 2 countries by organisational unit or location, 1-1 country by departments – by risk management portfolio.
- Armenia uses all categorisation.
- Bulgaria use a mixed solution: The audit universe could be categorised by departments/organisational units, by processes or combination of these two approaches.
- Croatia: it can be used all of them – it depends on entities; mostly they use by processes and by operational programmes.
- Georgia use another mix: by departments and processes.

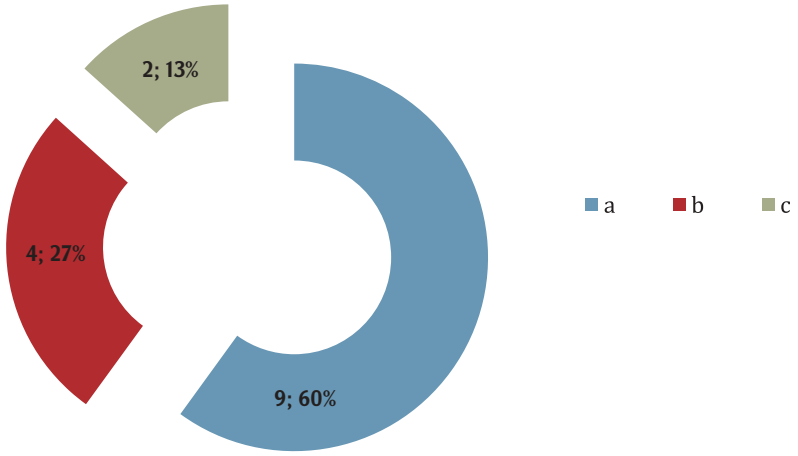
9. *Is there a requirement in your country for managers to carry out risk assessment as part of formal risk management procedures?*

Options:

a. Yes

b. No

c. It is required but few organisations actually have formal risk management procedures in place.



10. Are internal audit involved in identifying and assessing risks as part of this process?

9 out of 15 countries answered YES.

11. How do IA units identify risks?

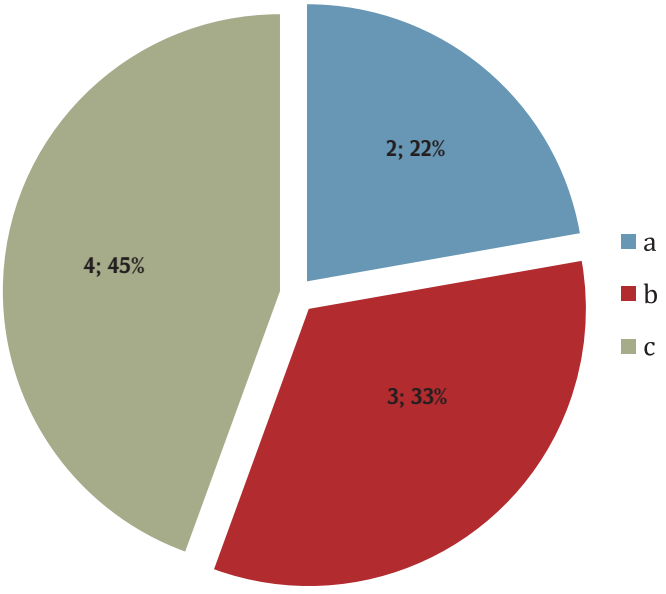
(This question was linked to Q10 – only those should have answered who had answered YES to Q11.)

Options:

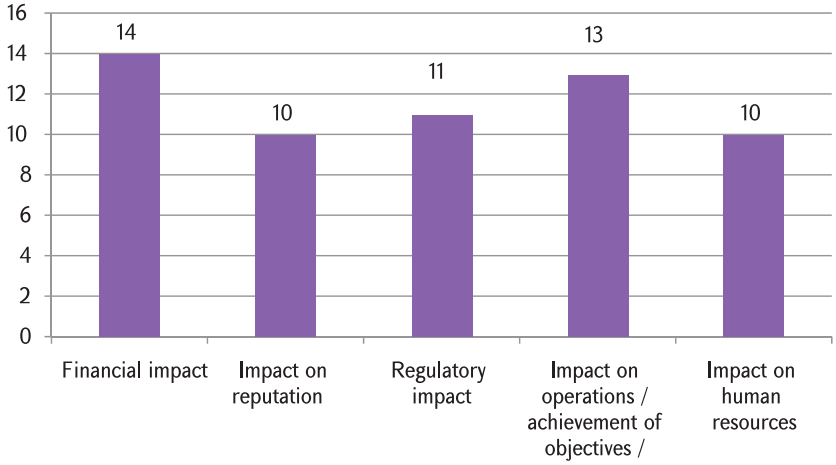
a. On the basis of risk register created as part of the risk management process by management

b. From risk registers made by internal auditors

c. In my country both above mentioned method are used – it depends on the given entity



12. What criteria are used by management or IA to assess the impact of identified risks?



- Bulgaria: The criteria mentioned above are most frequently used. The different entities and IA Units could define other criteria relevant to their specific activities.
- Croatia use an additional type: impact of non-reaching the set goals.
- Moldovan example: Materiality with a share of - 15 %; Control environment - 10 %; Sensitivity -10 %; MF' Management concerns - 15 %; Complexity of the process -10 %; Changes of people and of system -10 %; The integrity of the data processing environment - 5 %; The last audit mission - 15 %; The results of the last audit mission - 10 %.

13. How does management or IA score the impact of identified risks?

Please see responses on question 14.

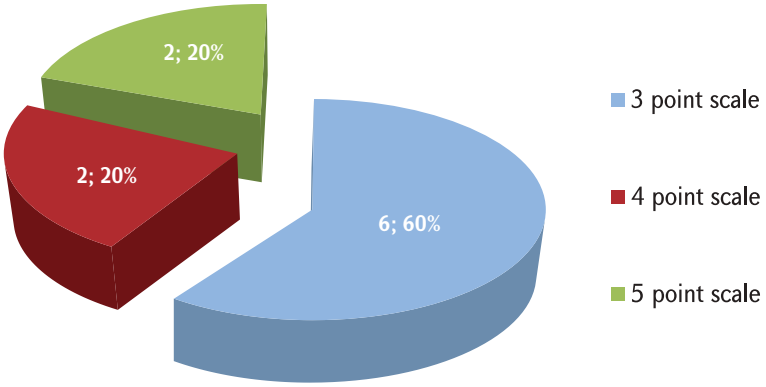
14. How does management or IA assess the probability of identified risks?

The options and the answers were the same in case of these two questions.

Answers:

- Bulgaria: The model of Risk Management Strategy for public sector organisations consists of 5 point scale for assessment of the impact of identified risk. This scale is not mandatory - the management is free to choose the point scale (3/4/5 etc.) which is most appropriate.

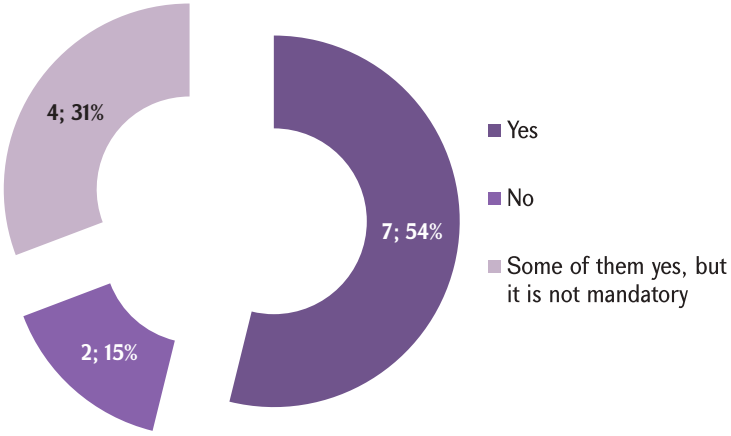
- Georgia: IAU are assessing each criteria/risk factor with its score, which is weather 3 or 4 point scale, at present IAU are not using impact and probability model.
- Romania: everyone can use a 3 point scale or 5 point scale, is not imperative.



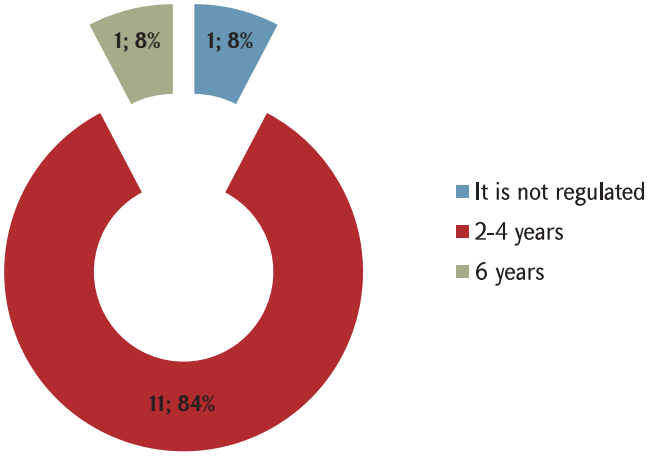
15. *What generic risk factors are used by IA units in selecting elements of the audit universe for examination?*

- In case of Georgia the following risk factors are used as well: Link of the system with other systems; Type and number of processes; Employees qualification & experience; External influence; Quality and proneness of internal controls.

16. Do IA units add a weighting to risk factors?



17. What period of time does the strategic plan should cover in your country?



It should be mentioned that 6 countries indicated that the strategic plan is for 3 years.

18. Which of the following areas are covered in the strategic audit plan in your country?

Options:

a. Objectives and performance indicators for the IA function, linked as appropriate to the strategy for the organisation

b. The methodology used to prepare the strategy and how the IA unit has assessed risks that impact the entity's objectives

c. How the IA unit will address the areas of most significance over a period of years (cycles of coverage for different elements of the audit universe)

d. The resources required and available to meet these needs and the impact of resource constraints on the ideal level of audit coverage

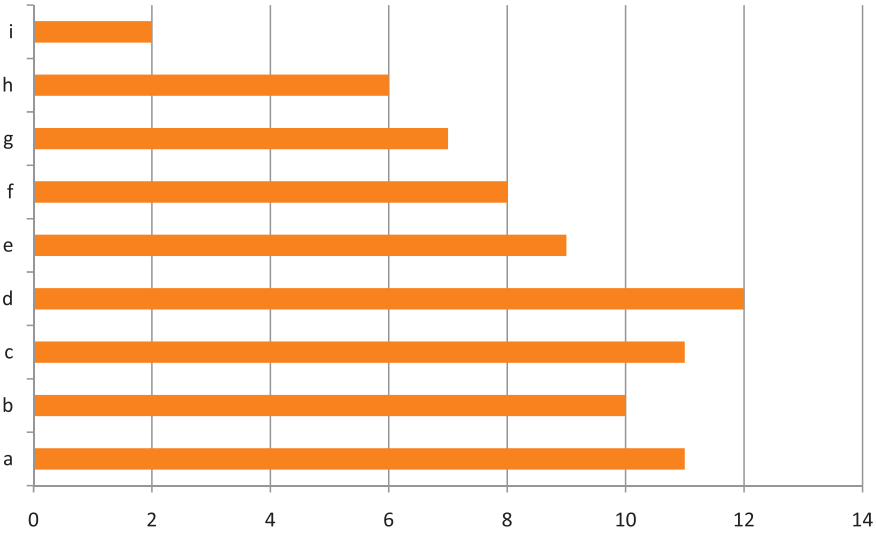
e. An internal risk assessment of those events which may impact the achievement of objectives in the audit strategy and mitigating actions to address such risks (for example, staffing shortfalls; skills shortages and training and other actions needed to address these risks.)

f. Plans for the coordination of work with other sources of assurance (e.g. external audit)

g. The approach for following up recommendations made

h. The higher or longer-term goals the IA function wants to achieve but may not achieve in the short term

i. Other(s)



19. What is the content of annual audit plan in your country from the followings?

Options:

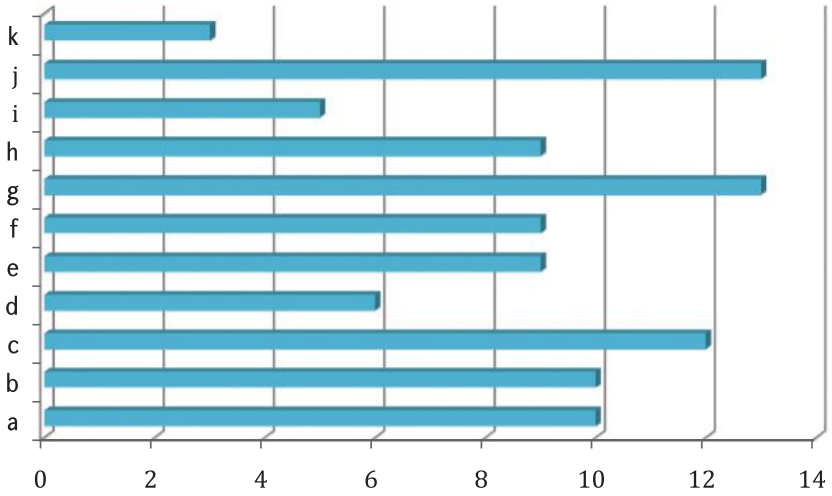
a. Relation between strategic objectives of the IA Unit and planned assignments

b. correspondence between planned assignments in the audit strategy and in the annual plan

c. Purpose, scope and duration of each audit assignment

d. Purpose and duration of each consultancy assignment

e. Allocation of staff
f. Resource situation including need for further resources, if necessary
g. Timing of assignments
h. Training plan
i. Budgetary resources
j. Time reservation for unplanned assignments
k. Other(s)



- Bosnia & Herzegovina: It contains a section on reporting, both on the regular annual reporting on the work of the unit's internal revisers, as well as periodic reports on the work of the internal audit unit.
- Croatia: Organisational position of Internal Audit Unit inside the organisation, changes in legislative, allocation of duties (how many audits will be performed by each auditor, how many meetings, education etc.).
- Georgia: Training plan and budgetary resources depends on IAU, some of them may add this topic in annual plan.