Introduction

Background and purpose of the guide

1. The Good Practice Internal Audit Manual Template, developed by the Internal Audit CoP of Pempal, defines the importance and the impact that an effective audit strategy and audit plan can have on meeting the overall goals, objectives and the mission of the internal audit unit. Planning provides a systematic approach to the internal audit work and requires knowledge and competency in a broad number of areas such as risk assessment and internal control.
2. This guide has been developed:
   - To help Internal Audit units produced effective risk based strategic and annual plans.
   - To provide a template of guidance on planning and risk assessment that could be made available by central units responsible for advising on the development on Internal Audit in their own countries.
3. The guide is fully consistent with the IIA standards on planning internal audit work. In particular:
   - **IIA Standard 2010** which requires "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals"
   - **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".
   - **IAA 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."
4. These standards require the Head of an Internal Audit unit to develop a risk-based plan. The Head of an Internal Audit unit should take into account the organization's risk management framework, including risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the Head of an Internal Audit unit uses his/her own judgment of risks after consideration of input from senior management and the board. The Head of an Internal Audit unit must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

Why is risk based planning important for an internal audit unit

5. The main problem faced by all 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 the audit universe (all the issues that an auditor might examine). The objective is to ensure that the Auditor examines subjects of highest risk to the achievement of the organisation's objectives.

6. Strategic and annual audit plans must be developed through a process that identifies and prioritizes potential audit topics. The entire population of potential topics, which can be categorized in many ways, is called **the audit universe**[i1]. 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**).

7. The audit strategy and annual plan are important documents, which are normally presented to management. The strategy 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 strategy 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 the first step in developing an excellent strategy.

How to use the guide.

8. The guide is presented in five chapters:

   - 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 likelihood and impact***" considers how to identify and assess risks in terms of their likelihood and impact on the organization'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

[1] See Chapter 3

- 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.

9. The guide contains generic guidance but also includes:

- Examples drawn from generic research on internal audit practice;
- Example of practices across PEMPAL countries (*depending on results of questionnaire*); 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 experience colleague.

Examples and general comments are highlighted in blue text or presented in blue boxes.

☑	*General hints and tips are presented in orange boxes*.

Chapter 1. Understanding risk-based audit planning

What are risks

10. The key definitions concerning risk are:

- ***Event.*** *An incident or occurrence, from sources internal or external to an entity, 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 an objective*
- ***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 organization successful in the achievement of its objectives or, if not well managed, will make the organization fail.*
- ***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 amount of risk, on a broad level, an organization is willing to accept in pursuit of its objectives.*
- ***Risk factors*** *is 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 audit planning risk assessment

11. Risks are considered by both Managers and auditors and are similarly defined[2].

- ***Risk management*** is (or should be) an integral part of internal control and is the responsibility of management. It is a structured process where managers (a) examine likely future events and the risks and opportunities

[2] 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.

these represent to the achievement of their objectives; and (b) determine and implement risk mitigation 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 risk factors that help prioritize work to areas of highest risk. The purpose of audit risk assessment is to ensure that audit resources are addressed to the audit of areas of highest risk to the organization.

☑	**No one can consider 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

12. 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. 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 as part of their planning process.
☑	Even where IA have to carry out their own risk assessment seek management input on such things as the organisation's appetite for risk
☑	An internal audit of risk management processes to encourage better risk management 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; 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 likelihood.

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 (likelihood) 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 audit planning risk assessment process.

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. Determining and categorising the audit universe.
1. Identifying events that may give rise to risks and opportunities to the achievement of objectives.	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*
2. Scoring events in terms of probability (likelihood) and impact to identify the level of **inherent** risk.	*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.
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).	*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.)*
4. Putting in place the risk mitigation action decided upon to arrive at an acceptable level of residual risk – this includes control activities.	*Auditors are not responsible for putting in place mitigation actions must assess the effectiveness of control activities in terms of its impact on* ***residual*** *risk.*
	3. Scoring events in terms of probability (likelihood) and impact (taking into account management actions to mitigate risk) to identify the level of **residual** risk.
	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)

18. 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 to determine areas that are high priority for examination.

20. The reason for this is obvious. With limited resources the auditor wants to concentrate audit work on areas where the risk exposure to the organization 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*

The actions required to implement risk-based planning

21. 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 (likelihood) 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 (likelihood) 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.*	
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 Categorizing the audit universe for risk based planning

What is the "audit universe"

22. The Good Practice 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 things that an internal auditor could separately examine.
- The universe consists of "***auditable objects***" which is a way of saying a 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

23. 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***.

24. 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.

25. 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 entity - that is 'horizontal' audits based on entire business processes. For example, an entity'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.

26. 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.

27. There is a high degree of commonality in the way that IA units in Government typically cut up or categorize the audit universe (see best practice examples).

Best Practice examples on categorisation of the audit universe	
From IIA Government survey	**From COP survey**
1. Almost all IA units have a formally documented audit universe (97%).	1.
2. The most common categorisations used are:	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%	•

28. Ultimately it is for the head of the Internal Audit Unit to decide how to categorize the audit universe and how many slices it makes sense to use. Most internal audit 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** (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** (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 aims, objectives and targets* ✓ *Guides to the entity's services* ✓ *Organisational charts or office directory* ✓ *Annual reports and any performance targets set for the entity* ✓ *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).* *Remember that you will present the categories in your audit strategy so they should be make sense to the managers of the organization.*

Seek senior managers' opinions

29. 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 entity's main objectives and the role of individual departments in achieving these
- Identifying the main risks they face in achieving the entity'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 entity priorities for assurance and audit attention.

Chapter 3 Identifying risks and assessing their impact and likelihood

30. Having identified the audit universe of auditable objects the next step in the process is to identify specific risks. The objective is for Internal Audit 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*

31. Best practice is that risk identification and risk assessment (scoring for impact and probability) should carried out in two stages. The reason is that the first stage (risk identification) is very similar to "brainstorming" where the objective is to capture all risks. However, the second stage 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 stages**. Use stage one to identify risks and stage 2 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 assess risks.

- **Where a risk management process is in place** Internal Audit 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** Internal Audit 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 organization. It will also be necessary to score events identified in terms of likelihood and impact to create and overall..

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

Identifying risks.

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

- Operational plans for the organization;
- Earlier reports by internal or external audit;
- Annual report of the organization;
- Major reviews of functions or activities carried out by management or by external bodies (e.g. World Bank 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 may be possible and will often be beneficial to carry out a joint risk assessment workshop with 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.*

36. 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 (Electric Gas water) No transportation Critical equipment/hard ware 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	Negative media publicity Levels of service below expectation Loss of trust from stakeholders because of operational shortcomings.

Assessing risks in terms of impact and likelihood.

37. Once all relevant events (risks) have been identified they need to be assessed and scored. Risk should be assessed 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. Assessing impact of risks is more complex than assessing likelihood but both are important elements of a risk assessment.

38. 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 criteria for impact and probability. Best 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).

Criteria for assessing impact

39. There could be many criteria for assessing risk impact but these should be limited to the four or five considered to be most important. The following **criteria for assessing impact** are commonly used and should be considered:

- ***Financial impact.*** The monetary consequences for the organization should the risk occur.
- ***Impact on reputation.*** The consequences with regard to the reputation of the organization, minister or even at a higher level the reputation of the entire country in the eyes of rating agencies, international donors, etc.

- ***Regulatory impact***. The occurrence of the risk may result in frozen budgets or programs or even in fines (e.g. EU funds).
- ***Impact on mission/ achievement of objectives/operations*.** The extent to which the mission of the organization may be impacted by the occurrence of the risk.
- ***Impact on people*** – unplanned loss of key people and skills can significantly impact organizations.

40. For each risk impact criteria the auditor needs to define what would represent different levels of impact (High, Medium high, Medium Low, 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 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.

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

Criteria for assessing likelihood (probability)

42. 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.

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

43. 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.

44. 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.

45. 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 and high risk.

46. 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 cans also be taken on which combinations to classify as low medium or high.

			LIKELIHOOD				
			Rare	Unlikely	Medium	Likely	Expected
			1	2	3	4	5
IMPACT	Low	1	Low	Low	Low	Low	Low
	Medium low	2	Low	Low	Medium	Medium	Medium
	Medium high	3	Low	Medium	Medium	High	High
	Very High	4	Medium	High	High	High	High

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

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

Chapter 4 Building risk-based strategic and annual plans

47. 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 can these risks be reflected in the audit strategy and annual work plan?

48. The objective of this stage of the process 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*".

49. 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

50. Most organisations use between five and eight risk factors. With less than five on average for Government internal auditors. All internal audit units surveyed by IIA use *degree of financial materiality* as one of the risk factors (see best practice table).

51. 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 fail in some way 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, organizational roles & responsibilities; clear ethical standards of behavior; 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 organization 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 Internal audit.
- **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; reorganization 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 quicker 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.
- **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. .*

Best Practice example - common risk factors used by Internal Audit units

From IIA Government survey	From COP survey
The most common categorisations used are:	2. 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%	•

52. 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 organization 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

53. 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 entity 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

54. 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, 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 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 High Medium or Low risk based on a suggest risk index score for example:

	Risk Index Score	**Risk/Priority**
	Over 45	High
	30-45	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 high medium and low categories.

55. 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.

☑	***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

56. A comprehensive strategic and annual plan of internal audit 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.

Strategic plan

57. 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 for what the IA function will achieve in the next 2-3 years.
- The methodology used to prepare the strategy and how the IA unit has assessed risks that impact the
- 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.
- 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.)
- The impact of resource constraints on the ideal level if audit coverage.
- Aspirational goals for what the IA function would like to achieve.

☑	***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 organization achieve it objectives. It can be useful way of generating support.*

Annual audit plan

58. The annual audit plan translates the strategic plan into the audit assignments to be carried out in following 12 months. It should define the purpose (title) 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.

59. In developing the Annual Plan, the head of internal audit 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 organization; 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.

60. 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

61. 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 organization. (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.).

62. Auditors must therefore monitor significant events that occur during the year 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

63. Planning is a dynamic process. New systems, more up-to-date information and other developments affecting the entity 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.

64. In reviewing the strategic audit plan, the head of internal audit should consider:

- changes that have occurred to the entity, 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 internal audit 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 internal audit 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

65. No plan is perfect. Changes are inevitable and may arise for many reasons:

- The entity may be reorganised,
- 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.

66. However, Heads of Internal Audit Units 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 programme. The results of this discussion should be documented.

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

68. Many internal audit units reserve a proportion of their resources for handing unplanned or ad hoc work. This is something that Heads of internal audit units 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 organizational 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 organizational 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 Organization. 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 Organization. Slow systems recovery.
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.	Organizational wide inability to continue normal business. Significant loss of operations. Widespread service interruption. Slow systems recovery.

Risk Assessment: Criteria for Risk Likelihood (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

69. The following example of a risk assessment methodology for use in planning internal audit work is based on the UK Government Internal audit Manual

70. 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

71. 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 entity 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

72. 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 entity. 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

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

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

74. 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

75. 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.

76. 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.