Contents

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.

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-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.*	

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.

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 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.

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.

☑ ***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

10

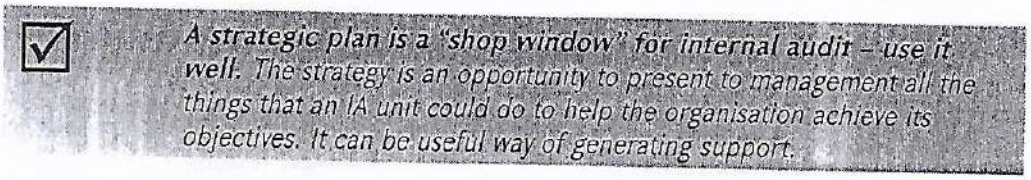
Chapter 5. Writing and updating strategic and annual plans

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.



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.

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

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.

AUDIT RISK

RELATED LINKS

The IAASB Clarity Project

Student Accountant hub page

Relevant to Papers FAU, F8 and P7

This article outlines and explains the concept of audit risk, making reference to the key auditing standards which give guidance to auditors about risk assessment

Identifying and assessing audit risk is a key part of the audit process, and ISA 315, *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*, gives extensive guidance to auditors about audit risk assessment. The purpose of this article is to give summary guidance to Paper FAU, Paper F8 and P7 students about the concept of audit risk. All subsequent references in this article to the standard will be stated simply as ISA 315, although ISA 315 is a 'redrafted' standard, in accordance with the International Auditing and Assurance Standards Board (IAASB) Clarity Project. For further details on the IAASB Clarity Project, read the article 'The IAASB Clarity Project' (see 'Related links').

WHAT IS AUDIT RISK?

According to the IAASB Glossary of Terms (1), audit risk is defined as follows:

'The risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated. Audit risk is a function of material misstatement and detection risk.'

WHY IS AUDIT RISK SO IMPORTANT TO AUDITORS?

Audit risk is fundamental to the audit process because auditors cannot and do not attempt to check all transactions. Students should refer to any published accounts of large companies and think about the vast number of transactions in a statement of comprehensive income and a statement of financial position. It would be impossible to check all of these transactions, and no one would be prepared to pay for the auditors to do so, hence the importance of the risk-based approach toward auditing. Traditionally, auditors have used a risk-based approach in order to minimise the chance of giving an inappropriate audit opinion, and audits conducted in accordance with ISAs must follow the risk-based approach, which should also help to ensure that audit work is carried out efficiently, using the most effective tests based on the audit risk assessment. Auditors should direct audit work to the key risks (sometimes also described as significant risks), where it is more likely that errors in transactions and balances will lead to a material misstatement in the financial statements. It would be inefficient to address insignificant risks in a high level of detail, and whether a risk is classified as a key risk or not is a matter of judgment for the auditor.

RELEVANT ISAS

There are many references throughout the ISAs to audit risk, but perhaps the two most important audit risk-related ISAs are as follows:

ISA 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with ISAs*

ISA 200 sets out the overall objectives of the auditor, and the standard explains the nature and scope of an audit designed to enable an auditor to meet those objectives. References to audit risk are frequently made by ISA 200, and the standard also requires that the auditor shall plan and perform an audit with professional scepticism, recognising that circumstances might exist that may cause the financial statements to be materially misstated. Professional scepticism is defined as an attitude that includes a questioning mind and a critical assessment of evidence.

ISA 315, *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*

ISA 315 deals with the auditor's responsibility to identify and assess the risks of

internal control, and the components of internal control systems. 14

3. Identification and assessment of significant risks and the risks of material misstatement

In exercising judgement as to which risks are significant risks, the auditor is required to consider the following:

- Whether the risk is a risk of fraud.
- Whether the risk is related to recent significant economic, accounting or other developments, and therefore requires specific attention.
- The complexity of transactions.
- Whether the risk involves significant transactions with related parties.
- The degree of subjectivity in the measurement of financial information related to the risk, especially those measurements involving a wide range of measurement uncertainty.
- Whether the risk involves significant transactions that are outside the normal course of business for the entity, or that otherwise appear to be unusual.

4. ISA 330 and responses to assessed risks

The requirements of ISA 330, *The Auditor's Responses to Assessed Risks*, will be covered in a future article, but essentially ISA 330 gives guidance about the nature and extent of the testing required, based on the risk assessment findings.

AUDIT RISK AND BUSINESS RISK

For the purposes of the Paper F8 exam, it is important to make a distinction between audit risk and business risk (which is not examinable in Paper F8), even though ISA 315 itself does not make such a distinction clear. ISA 315(2) defines business risk as follows:

'A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.'

Hence, business risk is a much broader concept than audit risk. Students are reminded that business risk is excluded from the Paper FAU and Paper F8 syllabus, although it is examinable in Paper P7.

THE AUDIT RISK MODEL

Finally, it is important to make reference to the so called traditional audit risk model, which pre-dates ISA 315, but continues to remain important to the audit process. The audit risk model breaks audit risk down into the following three components:

Inherent risk

This is the susceptibility of an assertion about a class of transaction, account balance, or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.

Control risk

This is the risk that a misstatement could occur in an assertion about a class of transaction, account balance or disclosure, and that the misstatement could be material, either individually or when aggregated with other misstatements, and will not be prevented or detected and corrected, on a timely basis, by the entity's internal control.

Detection risk

This is the risk that the procedures performed by the auditor to reduce audit risk to an acceptably low level will not detect a misstatement that exists and that could be material, either individually or when aggregated with other misstatements.

The interrelationship of the three components of audit risk is outside the scope of this current article. Paper F8 students, however, will typically be expected to have a good understanding of the concept of audit risk, and to be able to apply this understanding to questions in order to identify and describe appropriate risk assessment procedures.

Creating a Risk Management Checklist

16

written by: Jean Scheid • edited by: Michele McDonough • updated: 4/29/2013

What is a risk management checklist and how do you create one? As a project manager, this is a question you should ask and find the answer to. Jean Scheid provides us with tips on creating a risk management checklist.

- **Elements of a Risk Management Checklist**

In any type of project planning, risk management is a necessary tool. Risk management identifies and prioritizes risks , measures how harmful they can be, and develops a plan to deal with risks that are a threat to the project. Beyond creating a risk management plan, you should also create a risk management checklist. As you develop your risk management plan, including the risks and how they will be dealt with, a risk checklist should quickly tell you from past experience and forecasting if a risk area will evolve .

Scope of Work - The first part of your risk checklist should include questions and answers such as: Has the work been done before or is it something new? In essence, has an area in the work been identified in prior projects as a risk? If a task is a new task within the project, what risks may occur?

Project Resources - The second part of the checklist should deal with your resources. Do you have the right number of resources? Do your resources have the experience they need or do they have to be trained? How experienced are they and do they work well together? Again, if a resource risk is a potential problem, it should be identified on your checklist.

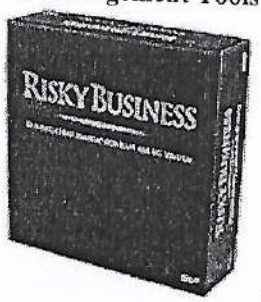
Project Timeline - The third part of your risk management checklist should identify items like scheduling conflicts and if they are flexible. Will you and your team have enough time to complete all the tasks within the project? If any items are identified as a risk, list them here.

Project Cost - This fourth part should identify risks that have to do with project costs and project overrun costs. If you feel a project may overrun its budget, list this as a risk on your checklist.

Outside Sources - What outside sources are involved in the project that may cause a risk? They are the fifth part of your checklist. If you feel an outside source can't deliver on time or has other issues that are considered to be a risk, put them on your checklist.

Deliverables - Can you deliver the project? That means not just the goals of the project, but the project itself. A goal may be to analyze tools to change a process and the project may be to change a certain process. If you feel the project has risk in its deliverables, identify this as a risk.

- **Risk Management Tools**



Understanding and using risk management in your projects requires processes and tools. Here at Bright Hub PM you can find many risk management tools to help you including:

How to Write a Risk Management Plan

Risk Management Plan: A Working Example

Is a Risk Management Plan Necessary?

Click on these templates for additional help:

HOW TO FOLLOW RISK ASSESSMENT PROCEDURES IN AN AUDIT

RELATED BOOK

Auditing For Dummies

By Maire Loughran

When performing an audit, you use risk assessment procedures to assess the risk that material misstatement exists. This step is very important because the whole point of a financial statement audit is finding out if the financial statements are materially correct.

A client's contribution to audit risk — the risk of a material misstatement existing in the financial records due to errors and fraud — influences your firm's plans regarding what audit evidence is necessary and which personnel will be assigned to the job. With higher risk comes the need for more involved audit risk procedures.

How exactly do you assess audit risk? You follow various risk assessment procedures: recognizing the nature of the company and management, interviewing employees, performing analytical procedures, observing employees at work, and inspecting company records. After you run through all applicable risk-assessment procedures, you use the results to figure out how high the chance is that your client has material financial-statement mistakes. Not every mistake is important.

- **Recognizing the nature of the company:** Here are some crucial questions to ask the client during your risk assessment procedures:
  - **What's the company's market overview?** For example, if the client is a bank, in how many states does it operate?

and understanding them can help you identify potential sources of inadvertent errors or intentional fraud that may affect the financial statements. Here are two real-life examples to consider:

- A payroll department objective is the accurate and timely processing of employee payroll payments. A risk associated with this objective is issuing inaccurate payroll payments.
- A tax department objective is to meet all legal and regulatory tax return filing obligations. Risks associated with this objective include filing returns that aren't materially correct and missing the filing deadline.

- **Analyzing processes and paperwork:** Put simply, analytical procedures test to see if plausible and expected relationships exist in both financial and nonfinancial data.

  Here are three common analytical procedures you do while assessing audit risk:

  - **Trend analysis:** You compare current financial figures to the same figures in the prior year.
  - **Ratio analysis:** Some common ratios are the current ratio, and inventory turnover.
  - **Reasonableness:** Does what you're seeing make sense based on other facts? For example, does the depreciation expense appear accurate when you consider the book value of all fixed assets on the balance sheet?

- **Observing the client at work:** One common type of observation is to watch the staff take a count of physical inventory. Visiting the company's business locations is another. Doing so gives you the opportunity to view the company's operations beyond what's in the books and records and to find out about the company's internal controls.

Annex 2 Systems Audit Procedures (design and operating effectiveness of Internal Control Systems)

2.1 *Audit Documentation and Evidence*

1 Audit Documentation (Working Papers)

The Auditor should in accordance with ISAE 3000, prepare audit documentation that provides:

- A sufficient and appropriate record of the basis for the auditor's report; and
- Evidence that the audit was planned and performed in accordance with ISAs and applicable legal and regulatory requirements.

Audit documentation or working papers means the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached. Audit file means one or more folders or other storage media, in physical or electronic form, containing the records that comprise the audit documentation or working papers for a specific engagement.

2 Audit Evidence

The Auditor should in accordance with ISAE 3000, ensure that audit evidence is gathered to support the Auditor's opinion and evidence that the audit was carried out in accordance with the IFAC *International Framework for Assurance Engagements* and *International Standard on Assurance Engagements ('ISAE') 3000* for *Assurance Engagements other than Audits or Reviews of Historical Financial Information.*

The Auditor should obtain sufficient appropriate audit evidence to support audit findings and to draw reasonable conclusions on which to base the audit opinion. The Auditor uses professional judgment to determine whether audit evidence is sufficient and appropriate taking into account the Contractual Conditions.

3 Retention of Audit Documentation (Working Papers)

The Auditor should retain audit documentation for the engagement (including evidence for audit fees and expenses such as invoices for hotel accommodation, air plane boarding cards, ticket stubs, time sheets etc.) for inspection by the Commission for a period of 5 years from the date of payment by the Commission of the Auditor's final invoice for this engagement. The Commission shall, on request and in accordance with the legislation in the country where the office having responsibility for the audit is based, have access to the audit documentation within this 5 year period.

4 Access to Records and Documents of the Entity

The Auditor should have full and unrestricted access at any time to all records and documents (including accounting records, contracts, minutes of meetings, bank records, invoices etc.), to employees of the Entity and to the Entity's locations insofar as this is possible and relevant to the audit of the Project. The Auditor may request the Entity to get access to banks (e.g. to request a bank confirmation), consultants and other persons or firms engaged by the Entity.

could have an adverse impact on the objectives of the Project. A deficiency in internal control exists when:

- An internal control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, errors and misstatements in the financial report for the Project on a timely basis; or

- An internal control necessary to prevent, or detect and correct, errors and misstatements in the financial report for the Project on a timely basis is missing.

Risk assessment involves an assessment of the risks that:

- the Financial Report of the Project is not reliable i.e. that it does not present , in all material respects, the actual expenditure incurred and the revenue received for the Project in conformity with applicable Contractual Conditions;
- the Project funds provided by the Commission have not, in all material respects, been used in conformity with applicable Contractual Conditions;
- fraud and irregularities can occur or have occurred which have an impact on Project expenditure and income and which are not detected and corrected in a timely manner;
- the relevant Contractual Conditions for the ~~Project are not complied~~ with. For this purpose the Auditor can concentrate on the controls and control areas described in the ToR Section 6.2 (Planning and Fieldwork, obtaining an understanding of the engagement context).

2.3 *Fieldwork*

1 Obtaining evidence regarding the design of controls

The scope of work should include an assessment of whether the **design** of the Internal Control System sufficiently mitigates the risks to the achievement of the Project (see point 2.2.4 above).

The Auditor should concentrate only on the key internal controls of the Entity and specifically those relating to the Project which are designed to prevent and detect material errors, irregularities or fraud with regard to the Project funding. The Auditor should determine which of the internal controls at the Entity were necessary to achieve the internal control objectives and assess whether these internal controls are suitably designed.

The Auditor should consider qualitative as well as quantitative factors but this audit is not a performance audit and therefore the Auditor should concentrate on financial internal controls rather than operational controls.

1) Evaluating the design of an internal control involves considering whether a control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting weaknesses and deficiencies.

2) Procedures to obtain evidence regarding the design of internal controls may include:

- Inquiring of Entity staff who may have relevant information;
- Evaluating whether descriptions of the Entity's internal controls, if available, fairly present the internal controls that have been designed and implemented;

3 Sampling and other means of selecting items for testing

When designing and performing tests of controls the Auditor may apply audit sampling or other means of selecting items for testing. Audit sampling involves the application of audit procedures to less than 100% of items within a population of audit relevance (e.g. a class of transactions or account balance) such that all sampling units have a chance of selection in order to provide the auditor with a reasonable basis on which to draw conclusions about the entire population.

Audit sampling can use either a statistical or non-statistical approach. The Auditor may use a judgmental selection of specific items from a population (e.g. high value or key items, all items over a certain amount, items to obtain information or items to test control activities). Selective examination does not constitute audit sampling.

While selective examination of specific items will often be an efficient means of obtaining evidence, it does not constitute sampling. The results of procedures applied to items selected in this way cannot be projected to the entire population; accordingly, selective examination of specific items does not provide evidence concerning the remainder of the population. Sampling, on the other hand, is designed to enable conclusions to be drawn about an entire population on the basis of testing a sample drawn from it.

4 Using the work of internal auditors

When the Auditor determines that an internal audit function is likely to be relevant for the audit he/she (a) determines whether, and to what extent specific work of the internal auditors can be used, and (b) if using the specific work of the internal auditors, whether that work is adequate for the purposes of the audit. The Auditor should comply with *ISA 610 'Using the Work of Internal Auditors'* insofar as this ISA is relevant to the audit.

5 Written representations

In assurance engagements other than audits or reviews of historical financial information (ISAE 3000) the auditor should obtain representations from the management. A written representation is a statement by the management provided to the Auditor to confirm certain matters or to support other audit evidence. The Commission does not require that the Auditor obtains written representations but this is recommended. The Auditor may request a letter of representation signed by the member(s) of the management of the Entity who have the primary responsibility for the Project and its financial aspects. The Auditor may request a letter of representation in cases where there is a specific point to obtain supplementary verification.

6 Fraud and irregularities

If Auditor may find that a fraud or irregularity has occurred or is likely to have occurred and such findings should be reported to the Commission in a complementary letter. The Commission will decide on follow-up measures including where appropriate the launching of an investigation by OLAF.

of the Entity's management and/or to carry out further audit procedures after the audit closing meeting and before the signature of the final report.

3 Procedure for the consultation and submission of the draft report

The Auditor should submit a draft report to the Commission (i.e. to the attention of the ATM) within 21 calendar days after the day of the closing meeting (i.e. the end of audit field work). The draft report should include the comments of the Entity insofar as these have already been obtained during the fieldwork of the audit and the closing meeting.

A paper and an electronic version of the draft report along with a cover letter should be submitted. The word 'draft' should be clearly indicated on all versions.

The Commission should provide comments on the draft report to the Auditor within 21 calendar days from receipt of the draft report. The ATM should collect the Commission's comments and ensure a proper and timely submission to the Auditor.

The Commission may request the Auditor to carry out additional audit work in which case a reporting deadline should be agreed on a case-by-case basis.

The Auditor should submit a draft report which takes into account the Commission's comments to the Entity (and a copy of that report with cover letter to the ATM) within 7 calendar days from receipt of the Commission's comments.

The Entity should submit comments to the Auditor within 21 calendar days from receipt of the draft report.

If the Entity's comments are not received within this deadline, the Auditor reminds the Entity until a written reply from the Entity is received. In the exceptional case where the Entity does not reply or where the absence of a reply leads to excessive delays in the consultation and reporting process, the Auditor contacts the Commission to discuss a solution. The Auditor should record and document causes and reasons for delays in the consultation of reports for which the Auditor is not responsible.

The Commission normally foresees a meeting with the Auditor after receipt of the draft audit report. This meeting will take place at DEVCO Headquarters in Brussels, or in the EU Delegation concerned by the audit or at another place whichever location is most appropriate and convenient for both parties. The purpose of this meeting is to discuss the draft report and any related issues that require specific attention. The Commission and the Auditor may agree to refer to alternative methods to discuss the report such as for example conference calls.

The Auditor may, where necessary or appropriate, propose a meeting with Commission and EU Delegation staff to discuss the draft report and the comments made thereon.

4 Procedure for the consultation and submission of the final report

If no additional audit fieldwork is required, the Auditor should submit a pre-final report to the Commission (i.e. to the attention of the ATM) within 7 calendar days from receipt of the Entity's comments on the draft report. The word 'pre-final' should be clearly indicated on the cover page of the pre-final report.

The Commission should inform the Auditor in writing whether it accepts the pre-final report within 14 calendar days from receipt of the pre-final report.