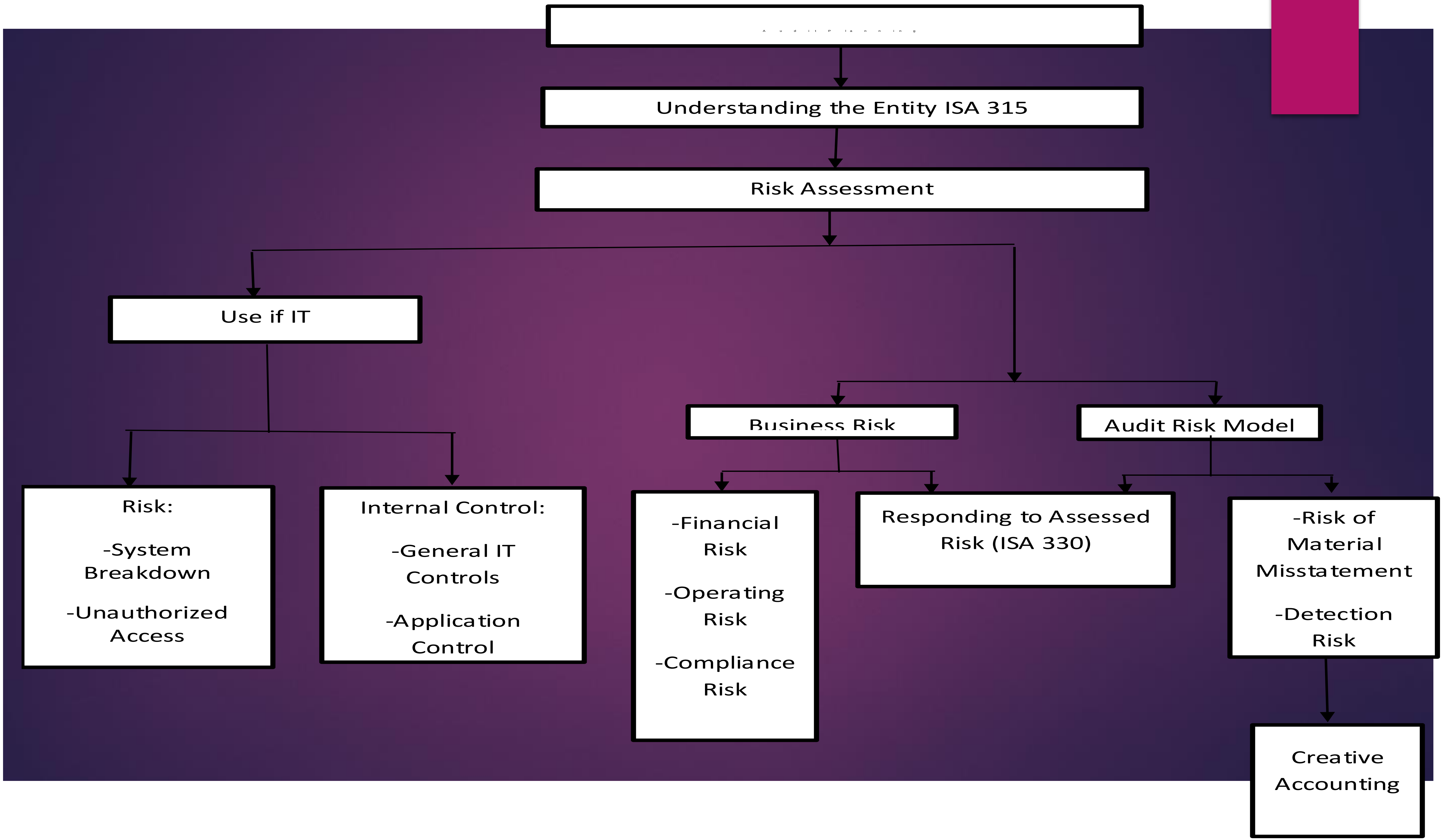
CONDUCTING RISK ASSESSMENT & AUDITING THE INTERNAL CONTROL SYSTEM

THE AUDIT QUALITY ASSURANCE WORKSHOP 7TH – 8TH MARCH 2017

Content:

- Risk Assessment Approaches During Audit
- Internal Control Environment: Auditing Internal Control System with bias of IT Environment
- Responding to Assessed Risks



Audit Planning

Understanding the Entity ISA 315

Risk Assessment

Use if IT

Risk:

-System Breakdown

-Unauthorized Access

Internal Control:

-General IT Controls

-Application Control

Business Risk

-Financial Risk

-Operating Risk

-Compliance Risk

Responding to Assessed Risk (ISA 330)

Audit Risk Model

-Risk of Material Misstatement

-Detection Risk

Creative Accounting

Understanding the Entity

Overview:

- The auditor obtains an understanding of the entity of the in order to assess the risks of material misstatement.
- Information will be sought regarding the industry in which the business operates and the business processes within the entity itself

Procedures

- ISA 315 states that ‘’the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity’s internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement’’.

A short Guide:

1. Understanding and identify risks arising from the entity and its environment, including relevant internal controls
2. Discuss risks amongst engagement team
3. Identify risk of material misstatement at the financial statement and assertion levels

- Assertions:

Classes of transactions

Occurrence, Completeness, Accuracy, Cutoff, Classification

Cont:

Account balances

Existence, Right and Obligations, Completeness, Valuation and allocation

Presentation and Disclosure

Occurrence, Rights and Obligations, Completeness, Classifications and Understandability, Accuracy and Measurement

4. Evaluate the design and determine the implementation of controls relevant to the audit and for risks which cannot be reduced to an acceptable level with substantive procedures only

5. Determine whether any risks are so significant that they require special audit consideration

❖ Document and Communicate Risk Assessment

Areas to gain an understanding:

- The ISA sets out a number of areas of the entity and its environment that the auditor should gain an understanding of:
- Industry, regulatory and other external factors
- Nature of the entity
- The entity's selection and application of accounting policies, including reasons for any changes
- Objectives, strategies and related business risks
- Measurement and review of the company's performance
- Internal controls relevant to the audit

Risk Assessment Approaches:

- Business Risk Model
- Audit Risk Model
- Use of Information Technology

Business Risk Model

Overview:

- Business risk is the risk arising to the business that it will not achieve its objectives
- Corporate governance guidelines emphasize the importance of risk management processes within a business
- The business risk model of auditing requires the auditor to consider the entity's process of assessing business risk and the impact this might have in terms of material misstatement

Business Risk

- Is the risk arising to entities that they will not achieve their objectives. It includes risks at all levels of the business.

Classification:

- **Financial Risks** – Risk arising from the company’s financial activities (e.g. investment risks) or the financial consequences of operations(e.g. receivables risks).

Examples: Going concern, market risks, overtrading, credit risk, interest rate risk, currency risk, cost of capital, treasury risks.

- **Operating Risks** – Risks arising from the operations of the business.

Examples: Loss of orders, loss of key personnel, physical damage to assets, poor brand management, technological change, stock outs, business processes unaligned to objectives.

Business risk

- **Compliance Risks** – Risks arising from non-compliance with laws, regulations, policies, procedures and contracts.

Example: Breach of company law, non-compliance with accounting standards, listing rules, taxation, health and safety, environmental regulations, litigation risk against client

Business Risk Management

Typically the process of risk management for the business is as follows:

- Identify significant risks which could prevent the business achieving its objectives
- Provide a framework to ensure that the business can meet its objectives
- Review the objectives and framework regularly to ensure that objectives are met

In practice, each of these stages is complex.

Audit Methodology

Principle behind the model

- ❖ ISA 315 requires that auditors consider the **entity's process for assessing its own business risks**, and the impact that this might have on the audit in terms of material misstatements.

Auditors consider:

- ✓ What factors lead to the problems which may cause material misstatements
- ✓ What the audit can contribute to the business pursuing its goals

The business risk audit approach tries to mirror the risk management steps that have been taken by the directors.

Impact on audit procedures

- **Tests of Controls** – as the auditor pays greater attention to the high level controls used by directors to manage business risks, controls testing will be focused on items such as the control environment and corporate governance rather than the detailed procedural controls tested under traditional approaches.
- **Analytical procedures** – Are used more heavily in a business risk approach, as they are consistent with the auditor's desire to understand the entity's business rather than to prove the figures in the financial statements.
- **Detailed testing** – The combination of the above two factors, particularly the higher use of analytical procedures, will result in a lower requirement for detailed testing, although substantive testing will not be eliminated completely.

Audit Risk Model

Overview:

- Audit risk is the risk that the auditors may give an inappropriate opinion when the financial statements are materially misstated
- The risk of material misstatement is made up of inherent risk and control risk
- The audit risk model expresses the relationship between the different components of risk as follows:

Audit Risk = Inherent Risk x Control Risk x Detection Risk

- Business risk forms part of the inherent risk associated with the financial statements
- Information gained in obtaining an understanding of the business is used to assess inherent risk
- Assessment of control risk involves assessing the control environment and control activities

Information Technology and Risk assessment

Overview:

- A huge number of organizations now use computer systems to run their businesses and to process financial information
- The main risks associated with using computerized systems include infection by viruses and access by unauthorized users. Both these risks could potentially have a very damaging effect on the business.
- This means that a number of the controls which the directors are required to put into place to safeguard the assets of the shareholders must be incorporated into the computer systems.
- Auditors have to assess the effectiveness of the controls in place within computer systems and can do this by performing a systems audit as part of their initial assessment of risk during the planning stage of the audit.

Risks associated with the use of computerized systems

The two key business risks of organizations using computerized systems are:

❖ The system being put at risk by a **virus** or some other fault or breakdown which spreads across the system

❖ The system being **invaded by an unauthorized user**, who could then:

✓ Affect the smooth operation of the system

✓ Obtain commercially sensitive information

Systems Audit

- ❖ As part of any audit, auditors are required to assess the quality and effectiveness of the accounting system. Increasingly, this necessarily includes a consideration of the computer systems in place within the organization.
- ❖ The following are the key areas they are likely to concentrate on to establish how reliable the systems are:
- ✓ Management policy
- ✓ Segregation of duties
- ✓ security

Internal controls in a computerized environment

- ❖ ISA 315 specifically requires the auditor to gain an understanding of the entity’s accounting systems and control environment as part of the risk assessment process at the planning stage of the audit. Today , almost any accounting system and control an auditor will encounter will involve some form of IT.
- ❖ There are two categories of internal controls:
- ✓ **General IT Controls** – Are the policies and procedures that relate to many IT applications at the same time. They support application controls by maintaining the overall integrity of information and security of data. Examples include procedure manuals, password protection and back-up facilities.

Cont:

- ✓ Application Controls – Are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. They are designed to ensure the integrity of the accounting records; that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data and numerical sequence checks with manual followup of exception reports.

Responding to Assessed Risks

Overview:

- Further audit procedures should be designed in response to the risks identified.
- As a result of the auditor's risk assessment and assessment of materiality an audit strategy will be developed in response. ISA 330 The Auditor's Responses to Assessed Risks.

Overall responses

- ❖ The auditor should determine **overall responses** to address the risks of material misstatement at the financial statement level.

This may include:

- ✓ Emphasizing to the audit team the need to maintain **professional skepticism** in gathering and evaluating audit evidence.
- ✓ Assigning more **experienced staff**, those with **special skills** or using **experts**
- ✓ Providing **more supervision**
- ✓ Incorporating **additional elements of unpredictability** in the selection of further audit procedures

Cont:

- The auditor may also make general changes to the nature, timing or extent of audit procedures, for example by performing substantive procedures at the period end instead of at an interim date. These decisions will take into account the auditor's assessment and understanding of the control environment.