Moderator :

Alukwe -

+254720474923|+254780474923

cakhonya@kabarak.ac.ke
alukchris@gmail.com

Information Systems Audit.

FIC4030 A

Day & Time:

- Saturday

09:00am – 12:00hrs

Planning IT Audit

- As technology becomes more ***integral to the organization's operations*** and activities, a major challenge for internal auditors is how to handle companywide **assessment of IT risks** and controls within the scope of their overall assurance and consulting services.

- Therefore, auditors need to understand the following.

✓ *Organization's IT environment.*

✓ *Applications and computer operations that are part of the IT infrastructure.*

✓ *How IT applications and operations are managed.*

✓ *How IT applications and operations link back to the organization.*

Planning an Audit

- Completing an *inventory of IT infrastructure components* will provide auditors with information regarding the infrastructure's vulnerabilities.

- The complete inventory of the organization's IT *hardware, software, network, and data components* forms the foundation for assessing the *vulnerabilities within the IT infrastructures* that may impact internal controls.

- Once an adequate understanding of the IT environment has been achieved, the *Chief Audit Executive (CAE)* and the *internal audit team* can perform the risk assessment and develop the *audit plan*

- **Factors considered when developing the audit plan,**

✓ *The organization's industry sector,*

✓ *Revenue size,*

✓ *Revenue type,*

✓ *Complexity of business processes,*

✓ *Geographic locations of operations.*

- *Two other factors having a direct impact on the risk assessment and in determining what is audited within the IT environment are its components and role they play.*

For example:

- ✓ *What technologies are used to perform daily business functions?*

- ✓ *Is the IT environment relatively simple or complex?*

- ✓ *Is the IT environment centralized or decentralized?*

- ✓ *To what degree are business applications customized?*

- ✓ *Are some or all IT maintenance activities outsourced?*

- ✓ *To what degree does the IT environment change every year?*

- *In addition to factors impacting the risk assessment, it is important for* CAEs (Chief Audit Executive) *and internal auditors to;*

1. *Use an approach that ascertains the* impact and likelihood of risk occurrence;

2. *Use an approach that links back to the business.*

3. *Use an approach that defines the* high, medium, and low-risk areas *through* quantitative and qualitative analyses

Planning An Audit

- IT changes may hinder the IT auditor's efforts to identify and understand the impact of risks.

- To help IT auditors overcome the above, CAEs can:

1. Perform *independent IT risk assessments every year to identify the new technologies that are impacting the organization.*

2. Become familiar with the *IT department's yearly short-term plans and analyze how plan initiatives impact the IT risk assessment*.

3. Begin each IT audit by *reviewing its risk assessment component.*

4. Be flexible with the IT audit universe — monitor the organization's IT-related risk profile and *adopt audit procedures as it evolves*

Planning An Audit

- Several IT governance frameworks exist that can help CAEs and internal audit teams develop the most appropriate risk assessment approach for their organization.

- **The Known set frameworks**;

1. *COBIT,*

2. *The UK's Office of Government Commerce.*

3. *IT Infrastructure Library (ITIL), and the*

4. *International Organization for Standardization's (ISO's) 27000 Standard series*

Assignment One

Audit Frameworks

Write a summary Notes under the following Audit Frameworks.

1. *COBIT,*
2. *The UK's Office of Government Commerce.*
3. *IT Infrastructure Library (ITIL), and the*
4. *International Organization for Standardization's (ISO's) 27000 Standard series*

Planning An Audit

- External audit planning is largely determined by the *audit requirements of the paying party.*

- Regulatory or contractual obligations also play a role in determining the scope of the external audits.

- The scope of an internal audit is usually more tactically focused on *high-risk areas or new and emerging risk areas.*

- The annual revisiting of sensitive or critical operations also is a common focus of internal audits.

1.Materiality

- Materiality is the concept of the relative significance or importance of a particular matter in the context of the whole organization.

- The assessment of what is material is a matter of professional judgment and includes the consideration of the effect of the error, omissions on the organization which may arise from control weaknesses identified during the audit.

- The auditor needs to consider the overall or aggregate level of error(s) acceptable to management *(the pain threshold),* and the potential result of the *cumulative effect of a number of smaller errors*.

2. Irregularities

- When planning an audit, the auditor is responsible for assessing the risk of fraud and incorporating the audit objectives and tests related to detecting irregularities.

- The category of irregularities such as fraud includes the following:

- ✓ *Acts that involve deception to obtain an illegal advantage*
- ✓ *Suppression or the omission of the effects of fraudulent transactions*
- ✓ *False recording of transactions without substance*
- ✓ *Manipulation, forgery, or falsification of records or documents*
- ✓ *Misappropriation or misuse of assets*
- ✓ *Acts that are noncompliant with existing agreements or contracts*
- ✓ *with third parties*
- ✓ *Errors arising from unauthorized access or use of IT systems*

Irregularities Cont…

- The audit planning should take the following into consideration to analyze any form of irregularities.

- ✓ *Corporate ethics*
- ✓ *Adequacy of supervision*
- ✓ *Compensation and reward structures*
- ✓ *Vacation scheduling policies*
- ✓ *The history of the organization*
- ✓ *Management turnover and competency*
- ✓ *Previous audit reports and legal activity*
- ✓ *The competitive environment of the business environment and condition*
- ✓ *of the control structures*
- ✓ *The complexity, sophistication, and maturity of the technical solutions*
- ✓ *being applied to the business processes*

Irregularities Cont…

- The auditor will need to develop an ability to think like a fraud perpetrator in order to successfully seek out and identify risk factors that may need to be investigated for proper levels of control.

4. Self-Assessment Audits

- This is an Audit process proffered *when the management culture is one that prefers to give guidance rather than evaluate compliance*.

- These *self-assessments* can range from a white paper documenting the best practices or guidelines that a process area agrees to abide by to a formal checklist of tasks that the management completes and submits to the audit department declaring their level of compliance*.*

4. Audit Staffing

- Part of planning IS audits involves making auditor assignments.

- Schedules, individual audit timing, and skill requirements must all be juggled to satisfy the plan requirements.

- Aligning the audit and technical skill requirements with the skills of the available staff and the development goals of the team members requires thought and management skills.

4. Audit Staffing Cont…

- The Auditor in Charge (AIC), who will lead the individual audit, must be *knowledgeable of the technology*, risks, and audit techniques unique to the subject and be able to provide guidance and developmental assistance for staff auditors assisting in the fieldwork.

- The AIC will be responsible for the final product and will approve all of the work papers, testing, and results.

5. Planning the Individual Audit

Once you have a particular audit assigned with a broad idea of the scope and the objectives defined, you will need to plan the audit.

Planning an audit involves the following:

- ✓ *Notifying the client and working out a schedule and pre-audit meetings*

- ✓ *Defining the scope and objectives.*

- ✓ *Determining the corresponding business processes on which to focus.*

Planning the Individual Audit Cont..

- ✓ *Understanding the process and its technical components*

- ✓ *Understanding and validating the inherent risks and threats of the processes and components with the client.*

- ✓ *Determining the desired controls or risk mitigants and validating expected controls and current residual risk with the client.*

- ✓ *Identifying management tools that would validate or report on the proper functioning of the controls*

Planning An Audit

Planning the Individual Audit Cont..

✓ *Performing a risk and control analysis to document the risk exposures and corresponding auditing priorities of the audit program components and their relevance to the scope and objectives*

✓ *Creating an audit program that incorporates the risk control analysis, gathers the evidence needed to determine the sufficiency of the existing controls and risk mitigants, and identifies the weaknesses.*

✓ *Finalizing staff resource and skill requirements*

✓ *Determining the time allocation for the components of the audit based on the materiality of the risks, the various tasks associated with testing each component, and the skill level of the staff.*

✓ *Establishing the framework of the work papers and fieldwork*

Planning An Audit

- Discuss in details the following concepts as involved in a modern Audit planning processes.

✓ Materiality.

✓ Audit Irregularities.

✓ Self assessment Audit.

✓ Audit Staffing.

- Provide an elaborate steps you would consider in an audit planning for Safaricom Bundle pricing system.

Questions ?

Lecture 4

Performing a Risk Assessment