AUI3703 – The internal audit process: Specific Audit Assignments and Reporting

Explain the terms governance, risk management and control

Governance is the process conducted by the board of directors to authorise, direct and oversee management towards the achievement of the organisation's objectives.
Risk Management is the process conducted by management to understand and deal with uncertainties (risks and opportunities) that could affect the organisation's ability to achieve its objectives.
Control is the process conducted by management to mitigate risks to acceptable levels.

Difference/differentiate between assurance and consulting services

Assurance services – An objective examination of evidence for the purpose of providing an independent assessment on risk management, control, or governance processes for the organisation. Examples may include financial, performance, compliance, system security, and due diligence engagements.
Consulting services – Advisory and related client service activities, the nature and scope of which are agreed with the client and which are intended to add value and improve an organisation's governance, risk management, and control process without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

CODE OF ETHICS

The purpose of the Institute's code of ethics is to promote an ethical culture in the profession of internal auditing and is based on the IIA's **definition of internal auditing (nature and scope):**
Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

The basic principles of the IIA's code of ethics

1. **Integrity** – The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgement. Integrity is the price of admission for internal auditors. It is so fundamental that, without it, an individual cannot serve as an internal audit professional.
2. **Objectivity** – Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgements.
3. **Confidentiality** – Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so. Management must have confidence that the internal auditor will not inappropriately disclose or use data in such a manner that harms the organisation.
4. **Competency** – Internal auditors apply the knowledge, skills and experience needed in the performance of internal audit services. There are specific standards requiring internal auditors to be competent and continuously strive for improvement.

How to formulate an audit procedure

Effectiveness

"To identify (formulation of audit procedure — can also use "to evaluate", "to inspect" or "to identify") factors that impeded the achievement of results (theoretical knowledge regarding effectiveness) throughout the XXX (e.g. manufacturing) department of ABC Ltd (application to question)"

- To identify
- To evaluate
- To inspect

Briefly describe qualities and abilities that a successful internal auditor should possess

- Curiosity
- Analytical qualities
- Qualities of persuasion
- Good business judgement
- Logical thinking
- Objectivity
- Good communication skills
- Good human relations
- Independence
- Self-confidence
- Initiative in developing techniques

Competencies needed to excel as an internal auditor

- Inherent personal qualities
- Knowledge, skills and credentials

THE PURPOSE AND NATURE OF VARIOUS FORMS OF INTERNAL AUDITING

- **Compliance audits**: Compliance can be defined as conformity and adherence to applicable laws and regulations as well as policies, plans, procedures, contracts or other requirements.
- **Financial audits**: During a financial audit, an internal auditor looks for evidence relating to the reliability and integrity of financial information. When such audits are conducted by an internal auditor, the information is normally intended to be used by management for internal decision-making purposes. The audit may include both operating and financial data.
- **Performance audits**: Performance auditing involves firstly determining management's objectives, then establishing whether the management controls that exist lead to effectiveness, efficiency and economy.
- **Environmental audits**: During a typical environmental audit, a team of qualified inspectors conducts a comprehensive examination of a plant or other facility to determine whether it is complying with environmental laws and regulations.
- **Fraud audits**: Fraud auditing involves assisting management in creating an environment that encourages the detection and prevention of fraud in commercial transactions.
- **Quality audits**: Quality auditing may be defined as a systematic and independent examination to determine whether quality-related activities are implemented effectively and comply with the quality systems and/or quality standards.
- **Programme results audits**: Programme results auditing is auditing the accomplishment of established goals and objectives for operations and programmes.
- **IT/IS audits**: IT audits come in a variety of forms. Any of the above types of internal audit could involve the use of computers or, for that matter, the audit of computer systems.
- **Application audits**: Application audits such as the auditing of inventory, payrolls, procurement, sales, treasury and other specific business functions have their own specific characteristics and the audit programme will typically involve a certain degree of standard audit tests.

TOPIC 3: PERFORMANCE AUDITING

The following terms may be regarded as synonyms for performance auditing:

- management auditing
- operational auditing
- value for money auditing
- functional auditing

Performance auditing and operational auditing address the extent to which a unit meets its performance objectives (effectiveness) and how well it uses resources (efficiency and economy).

THE COMPONENTS OF PERFORMANCE AUDITING

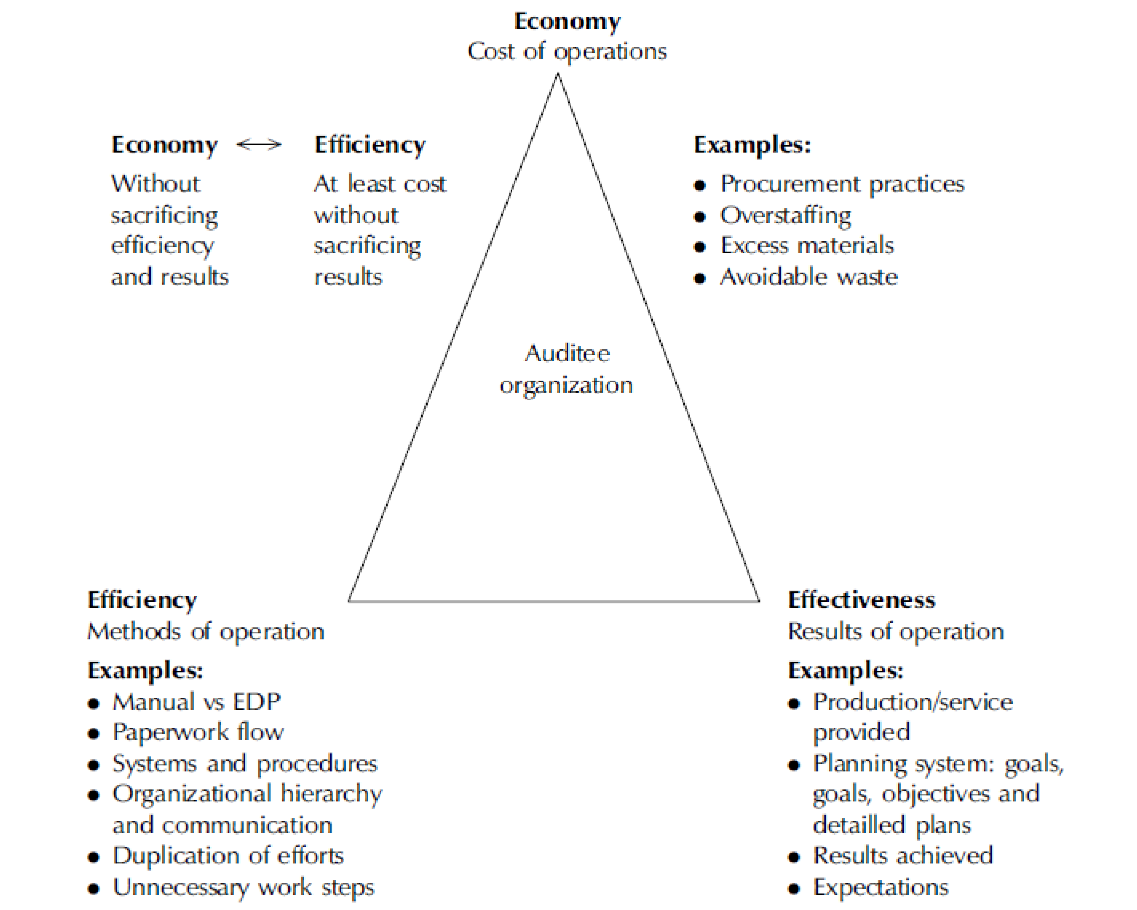
Performance auditing has four principal components, namely:

1. **Financial:** This component is concerned with proper and adequate accounting and reporting procedures. In operational auditing it is only one element of an audit assignment and it is made applicable to all the activities of an organisation.
2. **Compliance:** Compliance is usually dealt with in conjunction with the financial component. It comprises compliance with Acts, regulations and internal policy and procedures.
3. **Economy and efficiency:** This component involves the achievement of the optimum balance between costs and results. Costs should be cut to the minimum, but not at the expense of results, and at the same time productivity should be improved, but without incurring excessive costs.
   In an investigation into economy and efficiency the auditors analyse the way in which the organisation is applying its resources, namely human resources, facilities, equipment, materials and funds. The following aspects are included:
   - the purchasing policy of the organisation
   - material prices and service costs
   - staffing in relation to the functions that have to be performed
   - surplus stock on hand
   - use of more expensive equipment than necessary
   - prevention of losses and wastage of resources
   - division of projects into logically manageable tasks
   - efficiency and application of operating systems and procedures
   - efficiency of documentation flow
   - performance of unnecessary tasks or duplication of tasks
   - allocation of responsibilities and authority within an organisation
   - speed of production and completion time for projects

   Efficiency is the extent to which a process or activity has been optimised such that, all other things remaining constant,
   - its output has been maximised for a given amount of input, or
   - its input has been minimised for a given amount of output

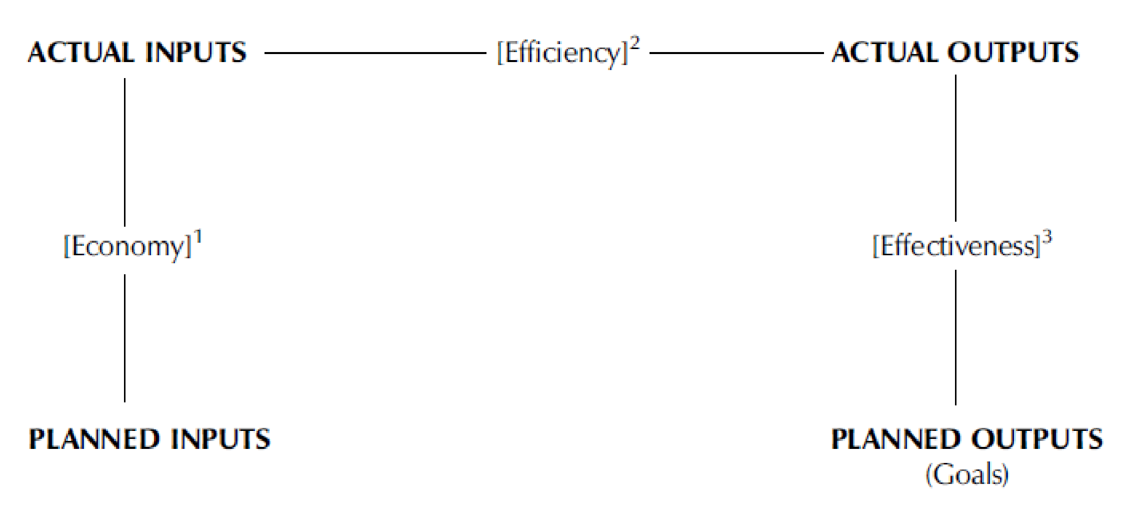
   Economy is the extent to which an organisation, unit or activity gets the right quantity and quality of a resource at the right time and best possible price.
4. **Effectiveness:** This component is concerned with the achievement of results and the resultant benefits. In an investigation of effectiveness internal auditors try to establish whether an activity is achieving its purpose and whether the results of an organisation or activity correspond to the targets set, the objectives or any other criterion. An investigation of effectiveness is concerned with quality rather than quantity. The following procedures would, for example, form part of an investigation into effectiveness:
   - evaluating the organisation's approach to the development of realistic targets and objectives and procedures for attaining those targets and objectives
   - evaluating the adequacy of management's method of measuring effectiveness
   - establishing the extent to which results are being achieved
   - identifying the factors that impede satisfactory performance or the achievement of results

DIAGRAM 1.2.2: THE OPERATIONAL AUDITING TRIANGLE



Source: Reider, HR. 1995. *The complete guide to operational auditing.*

DIAGRAM 1.2.3: THE THREE E'S



(1) Economy – the relationship between planned inputs and actual inputs in terms of unit costs

(2) Efficiency – the relationship between actual inputs and actual outputs

(3) Effectiveness – the relationship between actual outputs and planned outputs

Aspects that the internal auditor should attend to when evaluating economy

1. the organisation's procurement practices
2. prices of materials and services
3. staffing in relation to the functions to be performed
4. excess inventory on hand
5. using more expensive manufacturing equipment than is necessary
6. waste and loss of resources

e.g.: Audit objectives for assessing the economic and efficient functioning of DWARF's mechanical plant

1. To determine whether the organisation's policy on purchases will ensure the most economical and effective utilisation of resources
2. To determine whether the stock holding is economical without jeopardising the effectiveness of the mechanical plant
3. To determine whether losses and waste in the mechanical plant are minimised
4. To determine whether the activities of the mechanical plant are grouped in logical, feasible processes or tasks
5. To determine whether document flow and provision of management information throughout the mechanical plant are efficient

Audit procedures that could be followed to determine the effectiveness of the manufacturing process

1. Determine whether realistic goals and objectives have been set for the manufacturing processes.
2. Evaluate the approach followed by the management of Cuttglas to establish the targets and objectives for the manufacturing processes.
3. Evaluate whether there are adequate measures that the management of Cuttglas can use to evaluate the effectiveness of the manufacturing processes.
4. Evaluate management reports and interview management to establish the extent to which the results are being achieved.
5. Identify the factors that impede satisfactory performance or the achievement of results, and recommend ways to address these.
6. Evaluate the adequacy of policies and procedures put in place to achieve the objectives.

Audit procedures for each of the items listed in the question that will utilise that specific item and whether the purpose of each audit procedure will be to evaluate either the efficiency, effectiveness or economy of the plant

Audit Procedure	Purpose
Obtain evidence that management has put in place procedures to ensure that the performance objectives set for the department are achieved and that their achievement is measured.	Effectiveness
Compare current targets with the previous year's targets for both years in order to determine whether the department is meeting expected outcomes.	Effectiveness
Evaluate the adequacy of staff allocated to the department and whether the reporting structure allows for adequate delegation of authority.	Efficiency
Review the job descriptions and personnel allocation in order to identify positions that may be overburdened, duplication of effort, idol positions, etc.	Efficiency
Analyse the purchasing policy with regard to the purchase of promotional material and ensure that the policy is such that material can be economically procured.	Economy
Enquire from management why there are surplus promotional materials on hand.	Economy

PROBLEMS ASSOCIATED WITH PERFORMANCE AUDITING

1. Performance auditing makes high demands on human relations
2. Performance auditing requires special proficiency and skills
3. High cost of performance auditing
4. Management involvement in and support for performance auditing

Performance Objectives: A performance objective is a clear statement of what an organisation, unit or activity wants to achieve. When we talk about a performance objective, we automatically include its measure and standard. You must be able to measure the performance objective's level of achievement.

For which aspects of performance should performance objectives be set?

Performance objectives should address the quality and quantity of the output from an activity, the time taken to perform it and the cost. You can therefore set performance objectives for the following aspects of any activity:

1. quality (how well)
2. quantity (how many)
3. time (how soon)
4. cost (how much)

A performance measure is a yardstick against which the achievement of a performance objective can be determined. A performance standard is the minimum required level of performance. Performance standards define required performance.

The hierarchy of performance objectives

1. mission – the highest-level performance objective
2. unit performance objectives
3. key performance objectives
4. specific performance objectives

What is the mission of an organisation?

The mission is the ultimate performance objective of an organisation or unit. It conveys the reason for the organisation's or unit's existence and what it is trying to achieve.

Elaborate on the relationship between mission and performance objectives

The mission of the organisation is the reason for the existence of the company and gives expression to what the organisation wants to achieve.

The organisation's mission can be seen as its primary performance objective. A performance objective is a clear statement of what the company wants to achieve. All the performance objectives must be achieved if the undertaking wants to achieve its mission.

If a single performance objective is not achieved, the mission of the organisation is also not fully achieved. If the mission of the organisation can be compared to a completed puzzle, then the puzzle pieces are the performance objectives and the puzzle will only be complete if all the pieces are in place.

The mission statement

The mission statement is a clearly worded, concise statement of what the organisation is trying to achieve, how it intends to achieve it, and why.

Good performance objectives are:

1. measurable (quantitative)
2. specific
3. results (output) centred
4. realistic and attainable
5. time-bound

<u>In contrast to this, unsound performance objectives are:</u>

1. unmeasurable (quantitative)
2. general
3. minimum or unattainable
4. time-extended

<u>Assessing the performance objective component</u>

To be able to assess the quality of performance objectives, the internal auditor needs standards against which to compare the manager's objectives. These standards must be either "generally accepted standards" within the organisation or agreed on with the manager before the evaluation commences. Performance objectives should:

1. have three elements – an objective, a measure and a standard
2. be clearly stated and unambiguous
3. be consistent with higher level performance objectives
4. be relevant to the activity
5. relate to the quality or quantity of the activity's output, its cost or the time taken to produce it (quality, quantity, time and cost)
6. be realistic and achievable within the planning period, usually the financial year
7. be documented
8. be communicated to all staff that is involved in achieving them

<u>Assessing missions/ Steps to follow when evaluating mission statements</u>

When assessing the mission of the organisation, the internal auditor must first determine whether the mission has been established and communicated to all relevant parties.

If the mission has not been established the internal auditor need to report this and the potential impact to top management and/or the audit committee.

The internal auditor needs to assess the following:

1. That the mission statement has been formally defined. Without a mission statement the organisation will be without direction.
2. That the mission statement conveys the organisation's reason for existence. To assess this the internal auditor must have a good understanding of the organisation, particularly regarding its purpose. The internal auditor must report any shortcomings to top management.
3. That the mission statement has been translated correctly into performance objectives.
4. That managers are keeping their mission statements in line with the changing needs and wants of their customers.
5. In publicly funded organisations, that the organisation's reason for existence if still valid, customer's till have a genuine need for the service provided.

When assessing the quality of the organisation's mission, the internal auditor must exercise diplomacy. Managers don't take kindly to being told bluntly that their objective statement is wrong. Point out shortcomings and suggest improvements.

<u>THE ADVANTAGES OF PERFORMANCE AUDITING</u>

1. Identification of problem areas, the factors that cause the problems and alternatives that could improve the situation.
2. Reducing costs by identifying opportunities to reduce wastage and inefficiency
3. Identifying opportunities to increase income
4. Identifying undefined goals, objectives, policy and procedures
5. Identifying criteria for evaluating the achievement of the organisation's objectives and goals
6. Recommendation of improvements to an organisation's policy, procedures and structure
7. Evaluating the performance of individuals and sections within an organisation
8. Inquiry into compliance with legal requirements and the organisation's policy, objectives and procedures
9. Testing for the existence of unauthorised, fraudulent or otherwise irregular actions
10. Evaluation of management information systems and control systems

11. Identification of possible problem areas in future activities
12. Provision of an additional communication channel between people at the operational level and top management
13. Provision of an independent, objective evaluation of the organisation as a whole

PROBLEMS ASSOCIATED WITH PERFORMANCE AUDITING

1. Performance auditing makes high demands on human relations
2. Performance auditing requires special proficiency and skills
3. High cost of performance auditing
4. Management involvement in and support for performance auditing

The following factors should be considered when drawing up a budget for an operational audit:

1. The scope of the operational audit.
2. The regularity of the operational audit.
3. The nature of the business.
4. The effectiveness of management.
5. The benefits that may be generated by the operational audit.

STEPS IN THE CHOICE OF THE AUDIT FIELD

1. Identify and describe the problem
2. Collecting information and evidence
3. Evaluating conditions within the organisation
4. Obtaining the approval of management for the performance of the performance audit

AUDIT TECHNIQUES FOR EFFECTIVENESS

1. Examine existing documentation, such as policy and procedure manuals to establish whether criteria for measuring the performance of the administrative department has been formalised and whether they are accurate.
2. Analyse policy and procedures to establish whether they are clear and will lead to the achievement of the goals set by the management of the organisation.
3. Hold interviews with the XXXX and YYYY to determine whether they are informed about the organisation‘s mission, performance standards and measuring criteria and whether there are any issues that may hamper the achievement of objectives.
4. Analyse rates, changes and trends by performing analytical review procedures on the operations of the department.
5. Send questionnaires to the staff members, to determine factors which may hamper the achievement of objectives.
6. Interviews with management of the department to ascertain the achievement of objectives.
7. Review reports to determine compliance with policies and procedures and the achievement of objectives.

General audit techniques that the operational auditor can use, and how each technique can be used to audit the efficiency of the department

1. **Examine** existing documentation to analyse the way in which the department is applying its resources, namely human resources, facilities and equipment.
2. **Interview** the management and staff of the department to determine whether the staff in the claims department are overqualified, underqualified or suitable for the jobs they are performing.
3. **Analyse** policies and procedures with regard to personnel and ensure that the number of personnel in the claims department are adequate in relation to the duties they have to perform.
4. **Review reports** of management and ensure that the costs incurred are kept to a minimum.
5. **Observe** the activities of the claims department to ensure that no unnecessary tasks are being carried out.

6. **Observe** the activities to ensure that the procedures followed in the claims department are logical and cost-efficient.
7. **Compile** organograms and accompanying job descriptions to ensure that the authority structures among the staff in the claims department are clear and respected.
8. **Draw up flow charts** to analyse whether the tasks are carried out in a logical manner.
9. **Write** to clients to enquire whether the completion time of the claims process is adequate and satisfactory.
10. **Distribute questionnaires** to obtain information about the capturing and processing of claims that have been submitted.

AUDIT TECHNIQUES – GENERAL LIST

1. Observations/physical inspection (observing specific activities)
2. Interviewing/questioning (to obtain information on processes)
3. Flow charts (Systems flow charts can be prepared for the different processes that are investigated or to analyse the physical layout of work areas)
4. Analysis of ratios, change and trends (The relationship between different operational and financial information over different periods of time can be analysed and interpreted in order to identify problem areas).
5. Verification, routine control and vouching (Confirming the truth, accuracy, genuineness or validity of assertions by tracing them to relevant documentation).
6. Evaluating (The information gathered during the audit process must be analysed and professionally evaluated according to objectives and Standards. Compared existing guidelines and results, with standards set by the organisation or the industry.
7. Reviewing the existing documentation, for example policy and procedural manuals
8. Drafting organisational diagrams and accompanying job descriptions
9. Analysing policy and procedures with regard to personnel
10. Interviews with management and operational staff
11. Questionnaires to management or operational staff and questions in the audit programme
12. Telephone or written enquiries from outside parties, for example suppliers and clients
13. Reviewing transactions

Formulate ten (10) questions to put to organisation management to gain background information on the efficiency of the administrative department.

1. Are the **XXXX** processes divided into logically manageable tasks or are there areas where the processes could be improved?
2. What adjustments would you make to the **XXXX** processes in order to improve the manageability of the administrative processes? Provide details.
3. To what extent is the capacity of your machines and staff utilised?
4. In which areas do you experience capacity shortages?
5. Is your staff satisfied with their workload or have you received any complaints regarding this issue recently?
6. In which areas can documentation flow be improved to be more efficient?
7. Are there any areas where unnecessary tasks are performed or where tasks are duplicated? Provide details.
8. In which areas could the allocation of responsibilities and authority within the XXXX department be improved?
9. How does the speed of production and completion time for projects in your department compare to that of other departments in the industry?
10. What process is in place to minimise wastage?

Eight (8) audit procedures that can be used to determine whether equipment has been economically procured.

1. Analyse the purchasing policy of organisation with regard to the purchase of equipment and ensure that the policy is such that the equipment can be economically procured.

2. Evaluate the procedures followed when purchasing the equipment and ensure that the procedures followed are in line with the purchasing policy and that the equipment purchased was purchased at the best price. Specifically note the tender procedures, specification of the equipment.
3. Discuss the amount spent on procuring the equipment with management and ensure that there are valid reasons for the purchase of the equipment.
4. Ensure that cost-benefit studies were completed before the equipment were purchased.
5. Analyse the finance terms of the purchased equipment, for example was it bought on a hire-purchase agreement, for cash or with a loan. Ensure that the finance method used is the most beneficial for the company.
6. Review the capital usage schedules and ensure that equipment will be used optimally.
7. Ensure that the replacement policy provides for the economical use of equipment.
8. Ensure adherence to the purchasing and replacement policy.

TOPIC 4: FRAUD AUDITING

CATEGORIES, FORMS AND EXAMPLES OF FRAUD

1. **Misappropriation** takes place when a person to whom the responsibility for certain assets belonging to another party has been entrusted uses such assets or allows them to be used in any way that conflicts with the interests or instructions of the owner of the assets, usually with malicious or deceptive intent.
2. Misappropriation becomes **embezzlement** when any attempt is made to conceal the act of misappropriation, for example by offering false explanations or falsifying documents.
3. **White collar crime** is a term for fraud committed by a respected person or a person who enjoys high social status in the exercise of his or her profession.
4. **External fraud** takes place when people outside the organisation perpetrate fraud against the organisation.
5. The form of fraud in which computer programmes and computer-stored data are manipulated to abuse funds and other resources is known as **computer fraud.**
6. **Management fraud** is the deliberate manipulation of financial and other reports in order to mislead the users of the reports regarding the performance of management.

FACTORS AND REASONS THAT PROMPT PEOPLE TO PERPETRATE FRAUD

1. There is pressure on the individual, either internal pressure in the form of debt or a desire for riches, or external pressure in the form of pressure exerted by the organisation on management to achieve projected profit figures and budgets.
2. Uncontrolled access to organisational assets tempts employees to appropriate them for their own profit.
3. There are personality disorders. Most people generally prefer to be honest, but unfortunately there are the exceptions who prefer to be dishonest.

KEY PRINCIPLES FOR MANAGING FRAUD RISK

1. A fraud risk management programme should be in place
2. Fraud risk exposures should be addressed periodically by the organisation.
3. Prevention techniques should be established.
4. Detection techniques should be established.
5. A reporting process should be in place to ensure potential fraud is addressed appropriately.

FRAUD PREVENTION

Fraud prevention involves those actions taken to discourage the commission of fraud and limit fraud exposure when it occurs.

The responsibility of internal auditors in deterring fraud

The responsibility of internal auditors in deterring fraud is set out mainly in the internal auditing standards and is based on the requirement that internal auditors should exercise due professional care in the execution of internal audit assignments.

Management's responsibility for controlling fraud

Management should clearly indicate in written policies its commitment to fair dealing, its position on conflict of interest, its requirement that only honest employees be hired, its insistence on strong internal controls that are well policed and its resolve to prosecute the guilty.

FRAUD DETECTION

Practical considerations relating to the fulfilment of the internal auditor's responsibilities regarding the detection of fraud

The principal function of internal audit is to support management in the economic, efficient and effective achievement of their goals. To fulfil this function properly, the internal auditor should:

1. have sufficient knowledge of fraud to be able to identify the signs that point to the existence of fraud
2. be alert to conditions such as weaknesses in internal control that could allow fraud to be committed
3. have a knowledge of the procedures that should be followed when there is any suspicion that fraud has taken place

Knowledge of the procedures to follow when fraud is suspected

1. First, any internal auditor who is not the senior on the audit project should inform the supervisor or the internal auditor responsible for the internal audit project of his or her suspicion that fraud may have taken place.
2. The factors that point to fraud should then be evaluated to determine whether any further action is necessary and whether a fraud investigation should be instituted.
3. If the conclusion is reached that fraud may well have taken place, the managers concerned should be informed and the internal auditors can then recommend the investigative procedures they consider necessary.
4. Last, the cause of the possible fraud should be identified, suggestions for rectifying it should be made and the internal auditors should ensure that management either pays the necessary attention to the problem or accepts responsibility if they fail to tackle the problem.

Course of action the internal auditor should follow when fraud is suspected:

Before discussing the matter with anyone other than the audit supervisors, the internal auditor should do the following without delay:

1. Verify all information and vouchers to ensure that all the information is correct and can be proved.
2. Keep all information and suspicions confidential. Take full and accurate notes of everything that is done, but do this carefully.
3. Obtain and take possession of all documents that relate to the transaction and place them in safekeeping.
4. Evaluate similar transactions for a particular period to see whether there have been any repetitions of the incident and whether similar incidents have taken place.
5. Test all transactions made by the person suspected of fraud during a particular period.
6. Review all available information and carefully determine what occurred, study all evidence and decide what possible conclusions could be based on the information.

What the internal auditor should NOT do:

1. Do not jump to conclusions.
2. Do not make any accusations.

3. Do not entertain the idea that any specific person is involved in a crime
4. Do not get involved in an informal discussion about the information, not even with the other members of the internal auditing staff.

FRAUD INVESTIGATIONS

Difference between the objectives of a fraud investigation and the objectives of other internal auditing projects:

In a normal auditing project, the internal auditor's tasks consist of the following:

1. Looking for symptoms that indicate that problems may exist.
2. Looking for weaknesses in the system, or susceptibility of the system to problems.
3. Making recommendations for improving efficiency, economy and effectiveness.
4. Reassuring management.
5. Emphasising compliance with developed procedures and controls and improving them.

A fraud investigation is geared to detection. In a fraud investigation, the internal auditor's tasks involve the following:

1. Looking for evidence supporting an identified irregularity.
2. Determining the particulars of the irregularity.
3. Quantifying the loss or scope of the problem and the period in which it took place, the method used and the people involved.
4. Acting as a gatherer of information and evidence.

A general programme for fraud examiners should, at a minimum, include the following:

1. Collecting industry data
2. Financial analysis
3. Reviewing of internal controls
4. Evidence gathering
5. Evaluating
6. Reporting of findings to appropriate parties.

Evidence gathering: Techniques to be used to gather evidence about fraudulent activities. Examples are:

1. interviewing
2. internal control charts and visual comparisons
3. document examination
4. employee searches
5. investigation (close supervision of suspects during an examination period)
6. observation (spying or snooping)
7. undercover
8. specific items; collection of evidence related to the fraud

TOPIC 5 INFORMATION SYSTEMS AUDITING

What are the steps that should be followed when performing an IT audit? (5 steps)

- STEP 1: PRELIMINARY ACTIVITIES

Gather organisational information which will serve as a basis for creating the audit plan.

- STEP 2: AUDIT PLANNING PROCESS

The planning process involves identifying the tasks to be performed in the course of an audit, allocation of those tasks to specific auditors, deciding when a task should commence and quantification of the duration of each individual task based upon the auditor allocated.

- STEP 3: EVALUATION OF INTERNAL CONTROLS

Evaluate the five control components (COSO), evaluate general and application controls, and perform tests of control to determine effectiveness.

- STEP 4: FIELDWORK - AUDIT PROCEDURES

Perform audit procedures, gather audit evidence and perform audit sampling where applicable.

- STEP 5: COMPLETING THE AUDIT

All findings are disclosed in the audit report issued to management. For each finding recommendations should be provided.

Within the IT environment management should ensure that:

1. systems function as planned
2. that data integrity is maintained
3. information and data are confidential
4. that systems and information are available when needed
5. data is accurate, complete and valid
6. access to systems and programs are only granted to authorised users.

Controls in IT audit

- General controls: to control access to data and programs
- Application controls: to control access to specific program functions to ensure the validity of input, processing and output

Key indicators of effective IT controls include:

1. The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services;
2. Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors;
3. Ability to allocate resources predictably;
4. Consistent availability and reliability of information and IT services across the organisation and for customers, business partners, and other external interfaces;
5. Clear communication to management of key indicators of effective controls;
6. The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently;
7. The efficient use of a customer support centre or help desk;
8. Heightened security awareness on the part of the users and a security-conscious culture throughout the organisation.

The advantages of CAATS

General benefits

1. improved efficiency and effectiveness of individual audits and of the audit department
2. ability to evaluate a larger universe and increase audit coverage
3. increased analytical capabilities
4. improved quality of activities performed during the audit
5. consistent application of audit procedures and techniques
6. increased cost effectiveness through the reusability and extensibility of computerised techniques
7. improved integration of financial/information systems audit skills
8. increased independence from information systems functions and greater credibility for the audit organisation

9. greater opportunities to develop new approaches
10. better management of audit data and working papers

Benefits of using CAATS during the conduct phase:

1. Data analysis: Sampling, sorting, comparing and other tasks can be done quicker than manual.
2. Increased coverage: Due to the speed of sorting, comparing and trend analysis with computers, audit coverage is increased.
3. Better use of auditor resources: Allow auditors to spend more time on activities that require their judgement.
4. Improved results: The auditor is able to conduct a thorough analysis of transactions within shorter time frames which will result in improved results.

The disadvantages (or reasons for the non-use) of CAATS

1. Too costly to purchase and maintain.
2. Too technical and complex for non-IS auditors.
3. Client system and data compromised.

CONSIDERATIONS IN THE USE OF CAATS

The following conditions indicate that the use of CAATS may be appropriate:

1. lack of audit trails to trace transactions to final records or to source documents
2. computer printouts which are extremely voluminous and which make manual extraction, summarisation or sorting too time consuming or virtually impossible
3. where information is not available in a format suitable for manual use
4. where the volume of transactions is so vast that extensive testing (large samples) is necessary to obtain meaningful results
5. the extent of computerisation at the auditee – the more extensive the computerisation, the more desirable the use of CAATS
6. where the effectiveness and efficiency of the audit would be increased
7. where detection risk would be significantly decreased as a result of more extensive testing capabilities

The consequences of inadequate planning

The failure to plan adequately for the use of CAATS can result in

1. cost and time overruns
2. arriving at the wrong audit conclusion
3. failure to achieve the desired objective of the test
4. significant frustration to both the auditor and the auditee

IT Proficiency and Due Professional Care

Two attribute implementation standards specifically address the IT proficiency internal auditors must possess and the consideration they must give to using technology based audit techniques:

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

1220.A2 – In exercising due professional care, internal auditors must consider the use of technology-based audit and other data analysis techniques.

Assurance engagement IT responsibilities

Three Performance implementation standards specifically address internal auditor's assurance engagement responsibilities regarding information systems and technology:

2110.A2 – The internal audit activity must assess whether the information technology governance of the organisation supports the organisation's strategies and objectives.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organisation's information systems.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organisation's information systems.

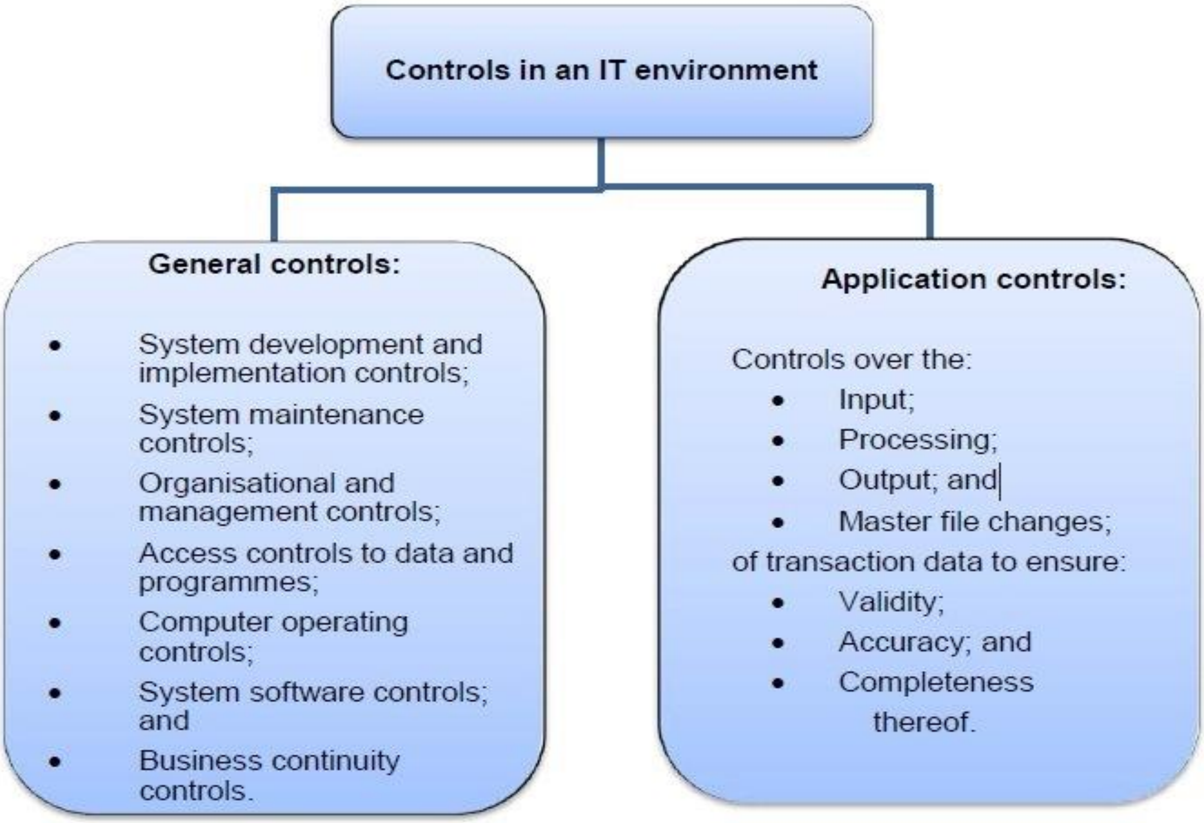
To fulfil the IT-related responsibilities, an internal audit function must:

1. Include the organisation's information systems in its annual audit planning process
2. Identify and assess the organisation's IT risks
3. Ensure that it has sufficient IT audit expertise
4. Assess IT governance, management and technical controls
5. Assign auditors with appropriate levels of IT expertise to each assurance engagement
6. Use technology based audit techniques as appropriate

These are the main categories of controls in an IT environment:

Certain controls fall under both general and application controls. Access controls apply to both categories, as illustrated below.

- **General controls:** to control access to data and programs
- **Application controls:** to control access to specific program functions to ensure the validity of input, processing and output



Controls in an IT environment

General controls:

- System development and implementation controls;
- System maintenance controls;
- Organisational and management controls;
- Access controls to data and programmes;
- Computer operating controls;
- System software controls; and
- Business continuity controls.

Application controls:

Controls over the:

- Input;
- Processing;
- Output; and
- Master file changes;

of transaction data to ensure:

- Validity;
- Accuracy; and
- Completeness

thereof.

Control structures must be designed to ensure:

1. Segregation of duties
2. Competence and integrity of people

3. Appropriate levels of authority
4. Accountability
5. Adequate resources
6. Supervision and review

RISKS ASSOCIATED WITH NEW OR DEVELOPED IT SYSTEMS

1. System development is a costly exercise. If it is not carefully planned and controlled, costs might get out of control. This could potentially put the company under severe financial constraint.
2. The new system might be susceptible to inaccurate or incomplete record keeping, for example the programs might contain errors.
3. Unacceptable or inaccurate accounting policies might be incorporated into the system or important accounting policies might not be incorporated at all. The system developers (eg programmers) might not understand the accounting policies and might implement them incorrectly.
4. The new system might not accommodate the needs of the users. The users might require certain functions that the new system is not able to perform.
5. When transferring information from the old system to the new system, information might be lost, duplicated or incorrectly transferred (with errors).
6. The new system might not have sufficient controls over access to information and the integrity of data.
7. If the new system is very complex, users might find the system useless if no one knows how to operate it.
8. In extreme cases, system deficiencies could result in temporary or even permanent business interruption.
9. The ability to commit fraud might be deliberately or accidentally designed into the system during its development.

Ten opportunities for the internal audit function to provide insight on IT Risks and Controls

1. Ensure IT risks are included in the annual risk assessment.
2. Provide insight to new systems development and IT infrastructure projects.
3. Integrate the review of IT audit in every audit.
4. Understand how IT can enhance internal audit productivity and control process throughout the organisation.
5. Provide control recommendations as new technology is deployed.
6. Educate management about emerging IT risks and controls that can be implemented to mitigate those risks.
7. Volunteer to pilot emerging IT projects to provide insight to control issues prior to deployment of new technology.
8. Employ IT specialists as subject matter experts for audit engagements involving extensive IT complexity.
9. Keep management and the board apprised of major IT risks that may impact the organisation.
10. Understand new technology that impacts the organisation regardless of whether the organisation currently employs it.

The five pillars of any security policy are the following:

1. **Authentication**. Users must be identifiable before they gain access to the system.
2. **Authorisation**. The user must have the necessary authority to get access to the system and the authority to use specific programmes and software within the system. Furthermore, the user must have the necessary authority to get access to specific information.
3. **Integrity**. The integrity of the information and the performance of the system should be protected. Users must be confident that processing will take place effectively and efficiently and that the results will be reliable.
4. **Confidentiality**. Users should know that access to certain programs and information is a privilege and they should be able to be trusted to use the information only for business purposes.
5. **Nonrepudiation**. There must be an audit trail so that the system can prove that the person who accessed as the user was actually the person doing the work on the system.

Risks associated with an internet connection

1. **Masquerade**: A normal attach where a user imitates somebody by using that person's login name and password in order to obtain additional privileges.
2. **Disclosure:** It is quite simple for someone to wire tap into a communication transmitted via the internet, including e-mail files and passwords.
3. **Unauthorised access**: Despite programmers' attempts, some internet software packages still contain vulnerable areas which make their systems vulnerable to attacks. On top of this, many of these systems are large, causing difficulties in their configuration and resulting in a large percentage of incidents of unauthorised access.
4. **Loss of data integrity**: One of the threats which is commonly overlooked is the modification of data while on a computer or in transit. The simple addition of the word "not" in a document, or the addition of several zeros at the end of an amount, is enough reason to cause chaos in the electronic trade.
5. **Refusal of service**: Refusal of service occurs when an internet network is flooded with data and/or requests which have to be serviced. This can cause the computer to stop functioning and be unavailable for any other purpose.
6. **Theft of services and resources**: Theft of services is a huge threat for those enterprises which offer special services to specific clients via the internet.

What is the difference between general controls and application controls?

IT general controls are those controls that are pervasive in nature and impact the overall technology environment. Information security controls to log on to a computer or overall disaster recovery plans are examples of general controls. Application controls are those controls that are specific to a particular system. Examples of application controls include input and output controls built into a specific software application.

What is the difference between physical access controls and logical access controls?

Physical access controls provide security over tangible IT resources and include such things as locked doors, surveillance cameras and security guards. Logical access controls provide security over software and information imbedded in the system and include such things as firewalls, encryption, login IDs, passwords, authorisation tables, and computer activity logs.

TOPIC 6: VARIOUS CONSULTING ENGAGEMENTS

The difference between assurance and consulting services:

Assurance services:

An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organisation. Examples may include financial, performance, compliance, system security and due diligence engagements.

Consulting services:

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organisation's governance, risk management and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation and training.

Types of consulting service:

1. advisory consulting engagements
2. training consulting engagements
3. facilitative consulting engagements
4. blended engagements

Selecting consulting engagements to perform

Consulting engagements are selected based on the magnitude of the associated risk or opportunity.

Sources of consulting engagements:

1. annual internal audit plan
2. requests from management
3. new or changing conditions

THE CONSULTING ENGAGEMENT PROCESS

Planning the advisory consulting engagement

1. Determine engagement objectives and scope.
2. Obtain final approval of objectives and scope from consulting engagement customer.
3. Understand the engagement environment and relevant business processes.
4. Understand relevant risks, if appropriate.
5. Understand relevant controls, if appropriate.
6. Evaluate control design, if appropriate.
7. Determine engagement approach.
8. Allocate resources to the engagement.

Performing the advisory consulting engagement

1. Gather and evaluate evidence.
2. Formulate advice.

Communicating and follow up

1. Determine nature and form of communications with engagement.
2. Give advice to engagement customer.
3. Conduct interim and preliminary engagement communications.
4. Develop final engagement communications.
5. Distribute final engagement communications.
6. Perform monitoring and follow up if appropriate.

TOPIC 7: REPORTING AND FOLLOW-UP ON THE COMPLETION OF AUDIT ASSIGNMENT

The basic objectives of internal audit reports are:

1. to supply useful and timely information on operational deficiencies and other aspects and
2. to suggest improvements in the way in which the organisation is run

The internal audit report therefore serves a twofold purpose, namely

1. to communicate the results of an internal audit
2. to persuade and call for action

The final internal audit report is basically merely a summary of the completed audit, documenting the following:

(1) what the internal audit team has achieved
(2) what was found in the course of the audit
(3) the extent of the deficiencies in the auditee organisation
(4) the steps taken by the personnel to rectify the situation

The audit report must be objective, clear, concise, constructive and timely.

Elements of an audit finding

Condition

- What was found?
- What was observed?
- What is not functioning effectively or efficiently and what is defective?
- Is the condition isolated or widespread?

Criteria

- What should the position be?
- What is the standard of comparison?
- What is the standard procedure or standard practice?
- Is it a formal or an informal procedure?

Cause

- Why did it happen?
- What was the underlying cause of the deviation?
- What caused the activities to become inefficient and uneconomic?

Effect

- What is the significance?
- What is the consequence of the finding?
- What will the final result be if the condition continues?

Recommendations

- What could be done to rectify the situation?
- What recommendations are practicable and reasonably acceptable?
- Who should implement the recommendations?

The basic characteristics of good internal audit reporting are the following:

1. Only important matters should be reported.
2. Internal audit reports should be useful and timely.
3. Internal audit reports should be accurate and should be adequately supported by vouchers.
4. The findings should prompt the management and personnel involved to take action.
5. Audit reports should be objective and should contain sufficient information to give their readers the necessary perspective.
6. Internal audit reports should be clearly and simply presented.
7. Internal audit reports should be concise.
8. Internal audit reports should have a constructive impact.
9. Internal audit reports should be logically arranged and positive.

The format of internal audit reports

A format that is flexible and comprehensive and can be used for any internal audit report that is not longer than four typed pages is the following:

1. management summary (if applicable)
2. background
3. overview
4. opinion/general evaluation
5. findings, recommendations and conclusions
6. comments by the auditee

If longer than 4 pages then an executive summary must be attached.

Weaknesses to look for in a report:

1. The date of the report is not stated. *The report should have a date*.
2. The report is not properly addressed. *The report should be addressed to the relevant interested parties.*
3. "…except those requiring executive approval." *Criteria for requiring executive approval must be explained.*
4. "During the past months…" *The exact date of the audit must be noted.*
5. The scope of the audit is vaguely outlined in the introduction. *Explain how the scope was determined or why it was limited.*
6. The purpose of audit is not clear. *The purpose should describe the audit objectives and may, where necessary, inform the reader why the audit was conducted and what the expected results were.*
7. Findings and opinion. *Findings should be based on criteria, conditions, cause and effect and opinions.*
8. Does not respond to original stated audit objectives
9. Does not indicate the procedures followed to arrive at the findings. *Criteria must be stated – what should exist.*
10. Does not clearly substantiate findings or explain significance of findings. *Audit findings emerge by a process of comparing what should be with what is.*
11. There is no indication of the sample method, error rate or confidence level used.
12. Does not explain the significance of the findings on late shipments. *Explain the risk or exposure.*
13. The report does not include positive remarks on procedures and controls that may be operating effectively.
14. The report is not signed. *Only a signed audit report may be issued.*