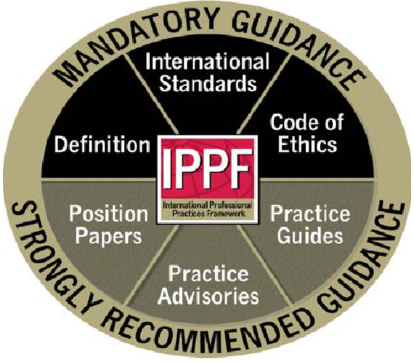
Topic 1: International Standards for the Professional Practice of Internal Auditing (IPPF)



Mandatory:

- The Definition of Internal Auditing
- The Code of Ethics
- The International Standards for the Professional Practice of Internal Auditing

Strongly recommended guidance:

- Practice Advisories (Implementation Guidance)
- Practice Guides (Supplemental Guidance, guidance on internal audit tools and techniques)
- Position papers

The Definition of Internal Auditing:
Internal auditing is an independent, objective assurance and consulting activity designed to add value to and improve an organisation's operations. It helps an organisation to accomplish its objectives by bringing a systematic, disciplined approach, to evaluate and improve the effectiveness of risk management, control and governance processes.

Assurance services
Traditional auditing services at various levels such as compliance, investigating & testing, performance evaluation
Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. There are generally three parties involved in assurance services: (1) the person or group directly involved with the entity, operation, function, process, system, or other subject matter – the process owner, (2) the person or group making the assessment – the internal auditor, and (3) the person or group using the assessment – the user.
EXAMPLES:
• The assessment that management's policies and procedures are adhered to.
• Examining whether control procedures are mitigating the risks identified.

Consulting services:
Objective is to support management in achieving their objectives
Consulting services are advisory in nature, and are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice – the internal auditor, and (2) the person or group seeking and receiving the advice – the engagement client. When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility.
EXAMPLES:

- Conducting control self-assessment training.
- Providing advice to management on risk management, control and governance issues.
- Assisting in developing and drafting policies.
- Process development
- Training
- Provision of advice

Principles – Code Of Ethics

Internal auditors are expected to apply and uphold the following four principles:
1. **Integrity** The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
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 judgments.
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.
4. **Competency** Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

Rules of Conduct – Code of ethics
1. **Integrity** Internal auditors:
1.1. Shall perform their work with honesty, diligence, and responsibility.
1.2. Shall observe the law and make disclosures expected by the law and the profession.
1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organisation.
1.4. Shall respect and contribute to the legitimate and ethical objectives of the organisation.

2. **Objectivity**
Internal auditors:
2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organisation.
2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. **Confidentiality**
Internal auditors:
3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.
3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organisation.

4. **Competency**
Internal auditors:
4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing (Standards)*.
4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

Purpose of the standards

- to outline basic principles that represent the practice of internal auditing as it should be performed
- to provide a framework for performing and promoting a broad range of value-added internal auditing activities
- to establish the basis for measuring internal auditing performance
- to promote improved organisational processes and operations

The standards consist of the following

  - Attribute standards
  - Performance standards
  - Implementation Standards.

- **Attribute Standards**
- o Attribute standards (the 1000 series) address the characteristics (attributes) of organisations and individuals performing internal audit activities. Attribute standards describe the attributes or characteristics needed for the effective administration of any internal audit activity.The 1000 Series
- o 1000:Purpose, Authority, and Responsibility
- o 1100:Independence and objectivity
- o 1200:Proficiency and due professional care
- o 1300:Quality assurance and improvement programme
- **Performance Standards**
- o Performance standards (the 2000 series) describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be measured. Performance standards deal with the actual execution (performance) of internal audits,
- o The 2000 Series
- o 2000: Managing the internal audit activity
- o 2100: Nature of the work
- o 2200: Engagement planning
- o 2300: Performing the engagement
- o 2400: Communicating results
- o 2500: Monitoring progress
- o 2600: Resolution of management’s acceptance of risks.
- The **Implementation Standards** expand upon the Attribute and Performance Standards, by providing guidance applicable to assurance or consulting activities and specific types of engagements

Three pillars of effective Internal Audit Services

- Independence and objectivity
- Proficiency
- Due professional care

Topic 2: Nature of and legislature pertaining to specific audit assignments

Forms of Internal Auditing (purpose & nature)

- **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.
Compliance tests.

Example

The focus of compliance auditing is on compliance with laws and regulations, statutes and internal policies. A compliance audit therefore sets out to discover how well a unit or organisation complies with an established set of "rules". Clearly, the level of compliance with formal rules is an aspect of performance. Although it is an important aspect, it is not the only one an auditor is concerned with.

- **Financial audits**

During a financial audit, an internal auditor looks for evidence relating to the reliability and integrity of financial information. Auditing of financial statements is directed at assessing the accuracy of financial reports relating to financial conditions and operating performance. Associated with an external audit
Substantive tests.

- **Performance audits**

Performance auditing involves firstly determining management's objectives, then establishing whether the management controls that exist lead to effectiveness, efficiency and economy.
An internal auditor must determine

- which key performance indicators are in use
- whether they are appropriate
- whether control objectives have been achieved

- **Environmental Audits**

Compliance 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.
A fraud auditor must know

- the realm of fraud possibilities (How can it happen?)
- the sources of information and evidence (Where do I look?)
- whether the environment is conducive to fraud (Is fraud likely?)
- the areas of fraud opportunity (Where can it happen?)
- the laws of evidence (How can I prove it?)

An internal auditor must be alert for red flags and indicators, such as personal behaviour pattern changes or substantial departmental growth or decline behind the norms

- **Quality Audits**

systematic and independent examination to determine whether quality-related activities are implemented effectively and comply with the quality systems and/or quality standards.
performed at predefined time intervals and ensure that the institution has clearly defined internal system monitoring procedures linked to effective action.
Quality audits can be an integral part of compliance or regulatory requirements.

- **Programme results Audits**

Auditing the accomplishment of established goals and objectives for operations and programmes.
Are the desired results being achieved?
Has management considered alternatives to achieve the same results at a lower cost?

- **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.

Qualities and abilities of an internal auditor

Curiosity.
The internal auditor should not take anything for granted. By asking questions and discovering the reasons for particular policies and procedures, the auditor gets to know the audit environment and acquires information that is of value in the operational auditing process.

Analytical qualities.
The ability to identify problem areas by rapidly examining a given situation and the ability to identify critical problem areas by distinguishing between material and nonmaterial aspects are important here.

Qualities of persuasion.
The success of an internal audit is measured by the extent to which the auditor's recommendations are implemented and implementation is directly proportional to the qualities of persuasion the auditor displays when conveying recommendations to management.

Good business judgment.
This quality depends on the knowledge and experience acquired by the auditor and includes the ability to view a problem from a manager's point of view and to ask appropriate questions. Internal auditors should be able to put themselves in the position of management, which may be difficult because the auditor is not likely to have personal experience of an operational management position.

Logical thinking.
Analysing an activity, identifying risks and weaknesses and making recommendations that could lead to the improvement of existing systems requires not only knowledge but also logical thinking. Only logical thinking can enable the auditor to make meaningful and practical recommendations.

Objectivity.
In the performance of any audit assignment objectivity is a basic requirement. Even if, for instance, the auditor was previously involved in an advisory capacity in the development and implementation of systems within an activity and irrespective of any personal relationships with any of the people working within an activity, the audit assignment should be approached objectively.

Communication skills.
The ability to communicate the results of an internal audit effectively is extremely important in ensuring that the shortcomings shown up by an operational audit are understood and effectively addressed by the auditee.

Good human relations.
Auditors must remain independent and cannot allow their opinions to be influenced by feelings of sympathy or of dislike or fear. The auditees are frequently unable to see any purpose in the audit. There is a greater degree of subjectivity involved in operational auditing than in other forms of auditing, which also increases the potential for conflict between the auditors and the staff.
Auditors need to understand human relations issues and be able to deal with them effectively.

Independence.
The internal auditor should be independent of the activity being audited. The auditor should therefore be able to carry out his or her task objectively and without restrictions. This enables the auditor to make impartial and unprejudiced decisions during the conduct of an audit.

Self-confidence.
Internal auditors should have sufficient self-confidence to counter the challenges posed by every operational audit. They should also carry out their task and present their opinions with the necessary self-confidence so that management will feel obliged to respond positively.

Initiative in developing techniques.
The unique nature of every internal audit requires the internal auditor to display initiative and creativity in the development of audit programmes, performance measurement techniques and better working methods that will achieve better results.

Flexibility
Ability to adapt quickly to new situations and challenges.

Work Ethic
Get the right things done the right way at the right time.

Integrity
The stakeholders must have confidence that internal auditors are trustworthy

Topic 3: Performance Auditing

Synonyms = Management, operational, value for money and functional auditing

Concentrates on evaluation of policy, procedures, division of authority, quality of management, effectiveness of methods, special problems and other aspects of an organisation's operations.

Purpose: Performance auditing aims at improving an organisation's **future performance** and it focuses mainly on management's policy, planning, control and decisions.

Independence: internal auditors:

- must not be involved in or be responsible for any operational matters within an activity which is being audited
- must be able to develop auditing programmes without being influenced
- must have full access to all evidence and members of staff wherever this is required for the purposes of the audit
- must be objective in collecting and evaluating information and evidence
- must be able to prepare audit reports on any matters which they consider necessary to report .

Reider's definition

Operational or performance auditing is an audit of operations performed from a management viewpoint to evaluate the economy, efficiency, and effectiveness of any and all operations, limited only by management's desires.

The elements of Reider's definition definition are as follows

1. **An audit of operations**

Performance auditing can be carried out in all functional areas of an organisation, such as marketing, sales, production and human resources. Performance auditing concentrates on the evaluation of policy, procedures, division of authority, quality of management, effectiveness of methods, special problems and other aspects of an organisation's operations.

2. **From a management point of view**

The principal focus of performance auditing is the achievement of management's objectives in the most economical, efficient and effective manner. For this reason it is important that a performance auditor should understand the way of thinking, objectives and concerns of top management in particular and focus on the aspects that are important to top management.

3. **Evaluation of economy, efficiency and effectiveness**

During an audit of economy and efficiency, the auditor looks at the optimum balance between costs and results. In an audit of effectiveness, the auditor determines whether an operation is fulfilling the purpose for which it was established.

4. **Any and all operating systems within an organisation**

A performance audit can focus on any component of an organisation, whether it is an operating unit, a functional area, a department or an activity within a department, where the audit objective amounts to reviewing the economy, efficiency and effectiveness with which management is achieving its goals.

5. **Only the needs of management restrict the scope of operational auditing**

As previously mentioned, performance auditing should focus on the aspects that are important to management. The freedom of the internal audit function to evaluate all the activities of an organisation should be incorporated in the internal audit mandate.

The aim of Performance Auditing

- Performance appraisal
- Identification of opportunities to make improvements
- Recommendations for the improvement of existing procedures and future action

The components of Performance Auditing

- financial
- compliance
- economy and efficiency
  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
- effectiveness
  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

Effectiveness is the extent to which an activity achieves its stated performance objectives. Effectiveness amounts to doing the right things. Doing the right things is about performing the right activities to achieve a performance objective. If you perform the right activities, you will achieve the performance objective and be effective. Improving effectiveness, will improve organisational performance.
Effectiveness – the relationship between actual outputs and planned outputs
Results of operation.

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
Efficiency – the relationship between actual inputs and actual outputs
At least cost without sacrificing results.
Method of operation.

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.
Economy – the relationship between planned inputs and actual inputs in terms of unit costs
Without sacrificing efficiency and results.

Aspects of the performance objectives

Audit objective: To determine ....

- quality (how well)
- quantity (how many)
- time (how soon)
- cost (how much)

Performance objectives – aspects of the business

- growing and developing the business
- producing and delivering services and/or products
- managing the relationships with stakeholders
- managing the organisation’s resources, for example finance, information, materials, equipment,

people or technology

Measuring achievement of performance objectives

- A performance measure is a yardstick against which the achievement of a performance objective can be determined. Identifying good or bad performance through performance standards
- A performance standard is the minimum required level of performance. By comparing actual performance with the required performance (standard), you can decide whether performance is good (above standard), bad (below standard) or acceptable (same as the standard).

The hierarchy of performance objectives

The decomposition of activities creates a hierarchy of performance objectives. You can define different types of performance objective according to their level in the hierarchy. For example, you could define four types:

- mission – the highest-level performance objective
  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.
- unit performance objectives
  A **unit performance objective** (UPO in diagram 1.2.4) is a clear statement of what a high-level activity within a unit is trying to achieve or what it is marketing or producing.
  Unit performance objectives must be supportive of and subordinate to the unit's mission.
- key performance objectives
  A key performance objective contributes to the achievement of its parent unit performance objective.
- specific performance objectives
  A specific performance objective contributes to the achievement of its parent key performance objective.

Good performance objectives are

- measurable (quantitative)
- specific
- results (output) centred
- realistic and attainable
- time-bound

Internal auditing standards applicable to Performance Auditing

- promoting appropriate ethics and values within the organisation
- ensuring effective organisational performance management and accountability
- communicating risk and control information to appropriate areas of the organisation
- coordinating activities of, and communicating information among, the board, external and internal auditors and management
- reliability and integrity of financial and operational information
- effectiveness and efficiency of operations and programmes
- safeguarding of assets
- compliance with laws, regulations, policies, procedures and contracts

The advantages of Performance Auditing

- Identification of problem areas, the factors that cause the problems and alternatives that could improve the situation
- Reducing costs by identifying opportunities to reduce wastage and inefficiency
- Identifying opportunities to increase income
- Identifying undefined goals, objectives, policy and procedures
- Identifying criteria for evaluating the achievement of the organisation’s objectives and goals
- Recommendation of improvements to an organisation's policy, procedures and structure
- Evaluating the performance of individuals and sections within an organisation
- Inquiry into compliance with legal requirements and the organisation's policy, objectives and procedures
- Testing for the existence of unauthorised, fraudulent or otherwise irregular actions
- Evaluation of management information systems and control systems
- Identification of possible problem areas in future activities
- Provision of an additional communication channel between people at the operational level and top management
- Provision of an independent, objective evaluation of the organisation as a whole

Problems associated with Performance Auditing

- Performance auditing makes high demands on human relations
- Performance auditing requires special proficiency and skills
- High cost of performance auditing
- Management involvement in and support for performance auditing

Steps in the choice of the audit field

- Identify and describe the problem
- Collecting information and evidence
- Evaluating conditions within the organisation
- Obtaining the approval of management for the performance of the performance audit

Audit objective: To determine ....

Audit procedure: To evaluate, to inspect, to identify + theoretical knowledge regarding audit procedure + application to question

Topic 4: Fraud Auditing

Definition of Fraud
Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial.
Elements of the crime
The elements of the crime are
(1)**misrepresentation**
(2) which causes or may **cause prejudice,** and which is
(3) **unlawful** and
(4) **intentional**

Categories and forms of fraud

- 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.
- Embezzlement: Misappropriation becomes **embezzlement** when any attempt is made to conceal the act of misappropriation
- white collar fraud: fraud committed by a respected person or a person who enjoys high social status in the exercise of his or her profession
- external fraud: people outside the organisation perpetrate fraud against the organisation.
- computer fraud: computer programmes and computer-stored data are manipulated to abuse funds and other resources
- management fraud: manipulation of financial and other reports in order to mislead the users of the reports regarding the performance of management.

Fraud Triangle

- Perceived need (Pressure)
- Perceived opportunity
- Rationalization

Red Flags

- Exhibit a lifestyle that appears to be well beyond their current means
- Have an unusual propensity to spend money
- Are experiencing extreme financial problems and/or have overwhelming personal debts
- Are suffering from depression or other emotional problems
- Appear to have a gambling obsession
- Have a need or craving for status and believe money can buy that status

Key principles for Managing fraud

- **Fraud risk governance (principle 1)**
  A fraud risk management programme should be in place
- **Fraud risk assessment (principle 2)**
  Fraud risk exposures should be addressed periodically by the organisation.
- **Fraud prevention and detection (principle 3 and 4)**
  Prevention techniques should be established.
  Detection techniques should be established.
- **Fraud reporting, investigation and resolution (principle 5)**
  A reporting process should be in place to ensure potential fraud is addressed appropriately.

Governance over the fraud risk management program

- Strong governance provides foundation for an effective risk management program
- Raise awareness and expectation of corporate behaviour and corporate governance practices
- Roles and responsibilities in a fraud risk management program must be communicated formally
- Components of a fraud risk management program
    - Commitment by board and senior management
    - Fraud awareness activities
    - Affirmation process that requires employees to affirm periodically that they understand and comply with policies and procedures
    - Conflict disclosure protocol – encouragement and help to disclose potential or actual conflict of interest
    - Fraud risk assessment that helps to identify reasonable fraud scenarios
    - Reporting procedures and whistle blower protection
    - Investigation process
    - Disciplinary and/or corrective actions
    - Process evaluation and improvement
    - Continuous monitoring

Fraud risk assessment

- Fraud risk identification
  Identifying the most comprehensive list of fraud risk scenarios. Elements that should be considered
    - Incentives, pressure and opportunities
    - Risk of management overriding controls
    - Population of fraud risks
    - Fraudulent financial reporting
    - Misappropriation of assets
    - Corruption
    - Other fraud risks
- Assessment of impact and likelihood of fraud risks
  Determining the potential **impact** and **likelihood** of each fraud scenario
- Response to fraud risk
    - Avoid: Risk is so intolerable that an organisation cannot even allow a single incident to occur
    - Reduce: organisation has little or no tolerance to a risk, but cannot avoid it without adversely affecting its objectives.
    - Share: an organisation desires to reduce the impact or likelihood of a risk, but does not have the skills or experience to do so effectively and efficiently it uses an organisation that is better equipped to execute the necessary controls.
    - Accept: the occurrence of a risk is tolerable.

Fraud prevention

- Organisational awareness
- Performing background investigations
- Providing anti fraud training
- Evaluating performance and compensation programs
- Conducting exit interviews
- Authority limits
- Transactional level procedures

Fraud detection

- Whistleblower hotlines
- Process controls
- Proactive fraud detection procedures

Fraud investigation and corrective action 8/27

- Receiving the allegation
- Evaluating the allegation

- Establishing investigation protocols
- Determining appropriate action

Implication for internal auditors

- Have sufficient knowledge
- Exercise due professional care; consider the probability of significant errors, fraud or non-compliance
- The chief audit executive must report periodically to the board on fraud risks
- The internal audit function must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk

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

Internal Auditing project	Fraud investigation
Looking for symptoms that indicate that problems may exist.	Looking for evidence supporting an identified irregularity.
Looking for weaknesses in the system, or susceptibility of the system to problems.	Determining the particulars of the irregularity.
Making recommendations for improving efficiency, economy and effectiveness.	Quantifying the loss or scope of the problem and the period in which it took place, the method used and the people involved.
Reassuring management.	Acting as a gatherer of information and evidence.
Emphasising compliance with developed procedures and controls and improving them.	

The practical performance of fraud investigations

1. Collecting industry data: This includes general information as to how the industry performs relative to financial and nonfinancial operations.
2. Financial analysis: Included here is financial analytical data for the organisation as compared to other organisations in the industry. Techniques that should be used are:
   - ratio analysis
   - vertical analysis
   - horizontal analysis
   - nonfinancial data (comparisons of different parts of statements, financial and operational, that should have a relationship)
   - cash flow information
   - net income adjustments (depreciation, receivables, amortisation tables etc)
3. Reviewing of internal controls: The determination that:
   - Transactions are executed as per management authorisation.
   - Transactions are properly recorded.
   - Safeguarding of assets.
   - Conformance of assets to records.
4. Evidence gathering: Techniques to be used to gather evidence about fraudulent activities. Examples are:
   - interviewing
   - internal control charts and visual comparisons
   - document examination
   - employee searches
   - investigation (close supervision of suspects during an examination period)
   - observation (spying or snooping)
   - undercover
   - specific items; collection of evidence related to the fraud
5. Evaluating: Analysis of evidence to determine if fraud actually occurred.
6. Reporting of findings to appropriate parties.

Communicating Fraud audit outcomes

- A brief clear statement of the issue
- A citation of the relevant policies, rules, standards, laws and regulations that may be applicable to

the case

- The analysis of the evidence gathered to form a professional opinion
- The conclusion; findings and recommendations

Topic 5: Information Systems Auditing

Steps in the IT Audit:

STEP 1: PRELIMINARY ACTIVITIES

- Gather organisational information
  - This information will serve as a basis for creating the audit plan.
  - The organisation's strategy and responsibilities for managing and controlling computer applications will be identified.
  - Obtain general data about the company, identify financial application areas and prepare an 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.
  - Quantification of the duration of each individual task based upon the auditor allocated.
- An audit should include
  - Tentative determination of the objectives and scope of the audit.
  - Determine overall business objectives of area to be reviewed as well as control objectives.
  - For each key performance area (KPA), performance objectives must be established.
  - Reviewing the design of internal control system for
  - stem and evaluation of the effectiveness of the implementation of the control system.
  - Selection of audit team.
  - Initial communication with auditees and others involved.
  - Preparations of preliminary audit program.
  - Planning of audit report.
  - Approval of audit approach.
- Structure of the plan
  - Preliminary survey – gain an initial understanding of the operations.
  - Internal control description and analysis – preparation of detailed descriptions of the internal controls relating to the area under review.
  - Expanded tests – tests that would be included in the final audit program.
  - Findings and recommendations – develop findings and recommendations to improve the internal controls.
  - Report production – includes documenting and communicating the final results.

STEP 3: EVALUATION OF INTERNAL CONTROLS

- Define internal control
  - COSO defines internal control as "a process, influenced by an entity's board of directors, management, and other personnel that is designed to provide reasonable assurance in the effectiveness and efficiency of operations, reliability of financial reporting and the compliance of applicable laws and regulations"
- Evaluate the five control components
  - *Control environment* – management's philosophy and operating style
  - *Risk assessment* – risk identification and analysis
  - *Control activities* – policies and procedures implemented in the organisation. The following controls should be implemented by an organisation:
    - preventive controls – controls intended to stop and error from occurring
    - detective controls – controls that detect whether an error has occurred
    - mitigating controls – control activities that mitigate the risks associated with key controls
  - *Information and communication* – Ensure that all important information is obtained and communicated throughout the organisation.
  - *Monitoring* – review output generated by control activities.
- Evaluation of general and application controls
  - General controls cover the entire CIS environment within which each set of application controls functions. General controls are related to all applications and provide a framework within which the CIS department exercises control over the development, operation and

maintenance of individual applications.
  - Application controls are user and programmed controls and are embedded in each of the data processing functions, namely input, processing and output.
- Tests of control
  - Determine the effectiveness of the operation of internal control.
  - Determine whether the design of the control is such that the control prevents material errors from occurring.
  - Assess how the control was applied, whether the control was applied consistently and who applied it.
  - The main focus is to re-perform the application of the controls themselves.

STEP 4: FIELDWORK - AUDIT PROCEDURES

- Define audit procedures
  - Tasks/audit tests performed by the auditor to gather evidence to ensure that the audit objectives are met.
- Audit evidence
  - Evidence is obtained to support the final conclusions of the audit.
  - Audit evidence should be reliable, sufficient, relevant and useful in order to support findings and conclusions.
  - All audit evidence should be documented to support findings.
  - The following procedures can be used to obtain audit evidence:
    - enquiry
    - observation
    - inspection
    - reperformance/calculation
    - monitoring/analysing
    - CAATs
- Audit sampling
  - Application of an audit procedure to less than 100% of the population in order to evaluate audit evidence.
  - Sampling risk is the risk that the conclusion reached may be different from the conclusion that would be reached if the entire population were tested.
  - Sampling objectives as well as the sampling method used must be documented in the audit working papers

STEP 5: COMPLETING THE AUDIT

- Reporting
  - All findings are disclosed in the audit report issued to management. For each finding recommendations should be provided
- Written reports
  - Refer to page 135 of the textbook for details on the requirements for a written report
- Basic audit report
  - The contents of the audit report includes the following:
    - Background, scope and objectives
    - Summary of major findings
    - Audit opinion
    - Detailed findings and recommendations
    - Acknowledgements of satisfactory performance
    - Detailed technical appendices
- Audit documentation
  - Working papers should include all of the following: notes, documents, flowcharts, correspondence, plans and results of tests, etc.
  - Working papers should support the findings and recommendations stated in the report.
  - Working papers should be evaluated by a partner or manager on the basis of the following: completeness, accuracy, appropriate findings and recommendations, follow-up to findings and recommendations
- Follow-up activities
  - The auditor should ensure that appropriate action was taken to address the findings raised in the report.
  - The nature, timing and extent of follow-up activities should be taken into account, as well as

the impact on the organisation if corrective action is not taken.

Definition of risk
The uncertain event that could influence the achievement of the organisational objectives.

Computer Risk

- Inherent risk - is the likelihood of a significant loss occurring before taking into account any risk-reducing factors.
- Control risk - is the likelihood that the control processes established to limit or manage inherent risk are ineffective.
- Detection risk - is the risk that if a material problem that would affect the conclusion pertaining to an audit objective has occurred, the auditors will not find it.
- This might arise because entries and activities are not fully examined.
- Audit risk - is the risk that audit coverage will not address significant business exposures.
- Audit risk consists of three components, namely **inherent risk**, **control risk** and **detection risk**.

Computer system threats
Threats may come from external or internal sources and may be intentional or unintentional as well as malicious or non-malicious. Internal threats may come from users, management, IS staff, IS auditors and others, acting alone or in collusion.

Top 10 Technology Risks issued as identified by the IIA advanced technology committee
1. Legislation and Regulatory Compliance
2. Threat / vulnerability management (Application exploits, viruses, Trojans, worms etc)
3. Privacy (including identity protection)
4. Continuous monitoring / auditing / assurance
5. Wireless security
6. Intrusion protection (firewalls, monitoring, analysis etc)
7. IT Outsourcing
8. Enterprise security metrics (dashboards, scorecards, analytics etc)
9. Identity management

Key components of modern information systems

- Computer hardware
- Networks
- Computer software
- Databases
- Information
- People

IT opportunities and risks

- IT Risks
  - Selection risk – selection of it solution that is misaligned with strategic objectives
  - Development/acquisition and deployment risk – unforeseen delays, cost overruns, abandonment of project
  - Availability risk – unavailability of system can cause delay in decision making, business interruptions, lost revenue, customer dissatisfaction
  - Hardware/software risk – business interruption, temporary or permanent damage or destruction of data
  - Access risk – unauthorised access can lead to misuse, malicious software modification, theft, destruction of data
  - System reliability and information integrity risk – errors or inconsistency may lead to irrelevant, incomplete, inaccurate or untimely information
  - Confidentiality and privacy risk – unauthorised disclosure of business partner's proprietary information or individual personal information may result in loss of business, lawsuits, negative press and reputation damage
  - Fraud and malicious act risk – theft of IT resources, intentional distortion or destruction of information may result in financial losses, misstated information

- Opportunities enabled by IT
    - ERP (enterprise resource planning)
        - Integration of business processes using a single operating database
        - Online real-time processing of transactions
        - Seamless interaction and sharing of information among functional areas
        - Improved process performance
        - Elimination of data redundancy and errors
        - Timely decision making
    - EDI (electronic data interchange)
        - Transaction processing efficiency
        - Fewer data processing errors

Components of IT Risk Management 7/11

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Control Activities

Within the IT environment management should ensure that:

- systems function as planned;
- that data integrity is maintained;
- information and data are confidential;
- that systems and information are available when needed;
- data is accurate, complete and valid; and
- access to systems and programs are only granted to authorised users.

Internal controls

It is the task of management, and not the auditor, to design and implement effective internal control systems in order to manage business risks and ensure that attention is paid to all aspects of control. The elements of management:

- planning
- organising
- directing
- controlling

Internal control is defined as the process designed and effected by those charged with governance, by management, and by other personnel to provide reasonable assurance about the achievement of organisational objectives regarding the following three categories:

- the reliability and integrity of financial reporting
- the effectiveness and efficiency of operations
- compliance with applicable laws and regulations

Internal control in a computer environment is achieved by implementing and maintaining **general controls** and **application controls.**

System of internal control

The objective of such a system of control is to ensure that -

• the computer system is properly developed, implemented and maintained

• proper controls are in place to ensure the **validity**, **completeness** and **accuracy** of transactions and data

General controls (control access to data & pgms)
- 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:
- Segregation of duties
- Competence and integrity of people
- Appropriate levels of authority
- Accountability
- Adequate resources
- Supervision and review

IT Governance: The leaderships, structure and oversight processes that ensure the organisation's IT supports the objectives and strategies of the organisation.

IT Governance controls integral component of overall governance.
IT controls at the governance level falls under jurisdiction of the board and senior management.
Senior management is responsible to conduct the control process on a day-to-day basis.
Includes:
- general policy on the level of security and privacy throughout the organisation
- Statement on the classification of information and the rights of access at each level
- A definition of the concepts of data and system ownership
- Personnel policies that define and enforce conditions for staff in sensitive areas
- Definitions of overall business continuity planning requirements

IT Management controls
Provides assurance that the organisation is structured with clearly defined lines of reporting and responsibility and has implemented effective control processes
IT controls at management level comprise standards, organisation and management, and physical and environmental controls.
Standards should cover:
- Systems development processes
- System software configuration
- Application controls
- Data structures
- Documentation

Aspects of IT Management controls
- Segregation of duties
- Financial controls
- Change management controls

IT Technical controls
Specific to the technologies in use within the organisations IT infrastructures
System software controls

- Access rights allocated and controlled according to the organisation's stated policy
- Division of duties enforced through system software and other configuration controls
- Intrusion and vulnerability assessment, prevention, detection in place and continuously monitored
- Intrusion testing performed on a regular basis
- Encryption services applied where confidentiality is a stated requirement
- Change management process
- System development and acquisition control
- Application based controls (validation)
  - Input controls
  - Processing controls
  - Output controls
  - Integrity controls
  - Management trail

Information security controls
Protection from unauthorised physical and logical access
Physical: locked doors, surveillance cameras and security guards
Logical: firewalls, encryption, login ids's, passwords, computer activity logs

Uses of Computer assisted audit tools and techniques (CAATS)

- to carry out various types of audit assignment
- in the execution of various types of audit procedure

The most important of these techniques, which are usually found in auditing software packages, are the following:

- the performance of the following procedures where only one computer file is used:
  - sorting or indexing of items
  - inclusion or exclusion of items
  - accounting computations
  - summarising of information
  - statistical sampling
- the performance of the following procedures in which two computer files are used:
  - the collation of information
  - the fitting or selection of information
  - the updating of information
  - the addition of information

The advantages of CAATS
General benefits

- improved efficiency and effectiveness of individual audits and of the audit department
- ability to evaluate a larger universe and increase audit coverage
- increased analytical capabilities
- improved quality of activities performed during the audit
- consistent application of audit procedures and techniques
- increased cost effectiveness through the reusability and extensibillity of computerised techniques
- improved integration of financial/information systems audit skills
- increased independence from information systems functions and greater credibility for the audit organisation
- greater opportunities to develop new approaches
- better management of audit data and working papers

Benefits during the conduct phase

- **Data analysis**. General audit software can be used to draw samples or to test 100% of the population because these tasks can be performed by the computer in a fraction of the time it would take to do them manually. Other tasks such as sorting and comparing can also be done more quickly by a computer.
- **Increased coverage**. It can take weeks to review systems containing millions of transactions manually, but with computers the auditor can analyse, sort and compare, and look for trends in thousands of transactions in minutes in order to increase audit coverage.
- **Better use of auditor resources**. Automation allows auditors to spend more time on activities in which they have to use their judgement.
- **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 nonuse) of CAATS

- **Too costly to purchase and maintain**. Some audit organisations believe that audit software is costly and cannot be proven to be cost effective. This may have been the case, but recently the costs have decreased substantially. Modern audit software is more flexible and can be used on a variety of applications.
- **Too technical and complex for non-IS auditors**. Modern audit software is more user friendly and can be used more freely without the assistance of programmers.
- **Client system and data compromised**. Previously audit software had to be loaded and run on the auditee’s computer system. Modern technology allows auditors to download the data onto their personal computer and analyse the data on the auditee’s premises.

CONSIDERATIONS IN THE USE OF CAATS

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

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

When an auditor first considers using CAATS in carrying out the audit process, the first step is to attend to the following factors:

- the computer knowledge, expertise and experience required to use CAATS
- the availability of suitable CAATS and suitable computer facilities
- whether it would be impractical to use ordinary (noncomputer assisted) audit techniques
- whether the effectiveness and efficiency of the audit process would be increased if CAATS were used
- the timing for the execution of CAATS
- the auditing software that will be used

CAATS can best be used for the following audit functions:

- Sorting and file reorganisation. Data can be sorted by date, customer name,department name etc.
- Summarisation, stratification and frequency analysis. Data can be summarised in account number order, departmental order and the frequency with which certain items are bought and used.
- Extracting samples, exception reporting, file comparison, for example current masterfile to prior year’s masterfile. These comparisons can be used to develop certain ratios to compare exceptions and deviations.
- Analytical review, for example extraction of ratios.
- Casting and recalculation.

- Examining records for inconsistencies, inaccuracies and missing data and creating reports.

PLANNING FOR THE USE OF CAATS

The auditor should consider the following specific planning items:

- knowledge of the auditee's business
- audit plan
- data file reconciliation

Knowledge of the auditee's business

With respect to the possible audit software, the auditor should consider accumulating the following information at the planning stage of the audit:

- the impact of the auditor's access to an auditee's data, hardware, software and networks
- the main systems of financial significance, and the data retention policies, related file layouts and volumes of transactions

Audit plan

The audit plan should be reviewed to ensure that optimum use is made of the available audit software. Appropriate resources should be available to support the audit plan.
Attention should be paid to the following aspects:

- need for continuity of staff on each audit to ensure that the use of audit software increases over time
- experience of scheduled audit staff in the use of audit software
- training requirements for audit staff before the fieldwork begins
- need for, and timing of, technical support
- specialised hardware or software required to access the auditee's data
- need for auditees to retain data necessary for the audit and to ensure that the auditor is made aware of changes in, for example file structures and content

Data file reconciliation

It is important to reconcile the auditee's data which are used for audit testing with the subject matter of the engagement, for example financial statements or auditee's control totals. The auditee should be asked to provide the information, such as control totals of the more important numerical fields, to ensure that all transactions were processed. It is also important to reconcile the number of records back to the source population.

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

- cost and time overruns
- arriving at the wrong audit conclusion
- failure to achieve the desired objective of the test
- significant frustration to both the auditor and the auditee

THE APPLICATION OF CAATS

- **Audit working papers**
  The audit firm's audit working papers document the audit programs and schedules, analysing account balances and significant classes of transactions in detail.
- **Substantive analytical procedures**
  - CAATS may be used to download information from the computerised accounting records of the auditee and then, using spreadsheets and modelling programs, the full range of analytical procedures may be performed.
  - CAATS may be used to analyse all journal entries processed during the period in order to identify all large and unusual journal entries for substantive testing. The auditor should be alert to the risk of management override of controls over non-standard journal entries and to the fact that there may be little or no visible evidence of such override.
- **Sample selection**
  Sampling software can facilitate the selection of random and other samples of source documents or transactions recorded.
- **Data sorting and analysis and printing of exception reports**
  CAATS may be used to sort data within the computerised accounts according to the specifications of the auditor, for example:
  - revenue transactions
  - payroll transactions
  - inventory listings
  - re-calculation

Auditing advanced and new IT systems
When a new system is developed, the following aspects of the IT system normally change considerably:

- hardware
- software
- personnel procedures
- documentation relating to the system
- controls

Risks associated with new or developed IT Systems

- 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.
- The new system might be susceptible to inaccurate or incomplete record keeping, for example the programs might contain errors.
- 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.
- 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.
- When transferring information from the old system to the new system, information might be lost, duplicated or incorrectly transferred (with errors).
- The new system might not have sufficient controls over access to information and the integrity of data.
- If the new system is very complex, users might find the system useless if no one knows how to operate it.
- In extreme cases, system deficiencies could result in temporary or even permanent business interruption.
- The ability to commit fraud might be deliberately or accidentally designed into the system during its development.

System failures as a result of poor development and implementation

- poor support from top management
- poor staff attitude
- unclear business objectives
- management and users unsure of their needs
- IT personnel unfamiliar with user needs
- additional user requirements not previously specified
- changes in user requirements
- organisational changes during the project
- failure to understand interrelationships between parts of the organisation
- over-optimistic file conversions
- poor quality input for file conversions
- poor documentation
- inadequate system and program testing

Purchased packages - Some of the advantages are the following:

- It can be installed immediately.
- The supplier of the package normally provides the relevant training.
- The supplier also offers some support
- The costs relating to the new system can be predetermined

Information Security (IS)

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Availability:** ensuring that authorised users have access to information and associated assets where required

Tools and techniques (controls) available in IT to manage risks

- information security policy
- identity and access management (IAM)
- encryption

Information system security policy

The policy covers the **hardware**, **software** and **information** found in the IT environment.

<u>These questions need to be answered when auditing the information security policy:</u>

1. Are there policies in place for managing and administering user identities and access activities?
2. Is there a strategy in place for addressing the risks associated with the IAM process?
3. Is there a reference model the organisation can use during the administration process?

The **five pillars** of any security policy are the following:

- **Authentication.** Users must be identifiable before they gain access to the system.
- **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.
- **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.
- **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.
- **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.

Information security tools and control techniques

Controlling access to computer resources

Identity and access management

The important questions to be addressed while implementing such a system are the following:

1. **Who has access to what information?** A decision needs to be taken as to who should have access to which resources, applications and information.
2. **Is the access appropriate for the job being performed?** Is the job description supported by the access given and is access given to a person which could be in conflict with and threaten the segregation of duties principle?
3. **Are the access and activity monitored, logged and reported appropriately?** The system should be designed in a way that supports regulatory compliance in the different environments. It should also facilitate the auditing process by logging all access so that it can be traced to ensure that only legitimate users have accessed the system.

Identity and access management is based on the following principles

- **Identity:** the element or combination of elements used to uniquely describe a person or equipment.
- **Access:** the information representing the rights that the identity was granted. These information access rights can be granted to allow users to perform transactional functions at various levels.
- **Access rights or entitlements:** the collection of access rights to perform transactional functions.

For identities to become part of the identity and access management system there are three stages that need to be followed, namely:

- **Provisioning.** Request, validate, approve, propagate and communicate the process. This should be in line with the security policy.
- **Identity management.** Monitor and manage passwords, audit and reconcile, administer policies and strategise or manage systems.
- **Enforce**: authenticate, authorise and log activities.

Encryption

- Data that are communicated between two computers or other devices should be secured against eavesdropping or even manipulation.
- One way to ensure the security of data is to use encryption.
- Cryptography is the name given to the use of mathematical algorithms to transform data. Its primary use is the protection of information.
- Encryption is a technique for turning messages into unreadable codes by scrambling up the data in such a way that the legitimate recipient can unscramble or “decrypt” the message easily, but an unauthorised recipient would only see garbage.
- The auditor needs to test the following:
  - That secure socket layer (SSL) communication protocol is used to secure sensitive information as it makes use of a two-key encryption standard.
  - That public key infrastructure (PKI) is utilised in conjunction with SSL.

Assurance engagement IT responsibilities

The internal audit function must:

- Include the organisation’s IT systems in annual audit planning process
- Identify an asses the organisation’s IT risks
- Ensure that it has sufficient IT audit expertise
- Assess IT governance, management and technical controls
- Assign auditors with appropriate levels of IT expertise to each assurance engagement
- Use technology-based audit technique as appropriate

Risks associated with an internet connection

- **Masquerade**: A normal attach where a user imitates somebody by using that person's login name and password in order to obtain additional privileges.
- **Disclosure:** It is quite simple for someone to wire tap into a communication transmitted via the internet, including e-mail files and passwords.
- **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.
- **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.
- **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.
- **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.

Topic 6: Various Consulting Engagements

Assurance service – reactive evaluation
Consulting service – proactive evaluation

Assurance services

- the assessment that management's policies and procedures are adhered to
- examining whether control procedures are mitigating the risks identified

The internal audit activity must evaluate risk exposures relating to the organisation's governance, operations and information systems regarding the:

  - Reliability and integrity of financial and operational information.
  - Effectiveness and efficiency of operations and programs.
  - Safeguarding of assets and
  - Compliance with laws, regulations, policies, procedures and contracts.

Consulting services

- conducting control self-assessment training
- providing advice to management on risk management, control and governance issues
- assisting in developing and drafting policies

In terms of **standard 2120** on risk management and consulting services:
2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.
2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organisation's risk management processes.
2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

The difference between Assurance and Consulting services

	Consulting	**Assurance**
Engagement parties	Involves 2 parties: 1) The person or group seeking advice – the engagement customer 2) The person or group offering advice – the internal audit function	Involves 3 parties: 1) The person or group directly involved – the auditee 2) The person or group making the independent assessment – the internal audit function 3) The person or group relying on the independent assessment – the user
Application of standard	Attribute and performance standards apply equally	Attribute and performance standards apply equally The applicable implementation standards are more stringent and numerous, because of more complex relations.
Engagement purpose	Providing advisory, educational or facilitation services Provide the greatest opportunity for insight	Providing independent assessment
Engagement communication	Communication varies based on the agreed scope and purpose of the engagement Formal or informal	Prescribed audience Include both auditee and 3-party Format is relatively standardised

The consulting engagement process

- Planning the advisory consulting engagement
    - Determine engagement objectives and scope.
    - Obtain final approval of objectives and scope from consulting engagement customer.
    - Understand the engagement environment and relevant business processes.
    - Understand relevant risks, if appropriate.
    - Understand relevant controls, if appropriate.
    - Evaluate control design, if appropriate.
    - Determine engagement approach.
    - Allocate resources to the engagement.
- Performing the advisory consulting engagement
    - Gather and evaluate evidence.
    - Formulate advice.
- Communicating and follow up
    - Determine nature and form of communications with engagement.
    - Give advice to engagement customer.
    - Conduct interim and preliminary engagement communications.
    - Develop final engagement communications.
    - Distribute final engagement communications.
    - Perform monitoring and follow up if appropriate.

Skill and experience required in performing consulting services

- Exhibit facilitation and collaboration skills
- Demonstrate both broad business experience and specific subject matter expertise (eg. Accounting, technology, regulatory)
- Build relationships quickly and demonstrate strong interpersonal skills
- Think analytically and solve unstructured problems
- Learn and adapt quickly in a dynamic environment
- Process information and respond quickly to requests
- Articulate and communicate results quickly, whether though presentation, written communication or oral communication.

Audit working paper preparation techniques to consider:

- Each engagement working paper should identify the engagement and describe the contents or purpose of the working paper.
- The internal auditor performing the work should sign (or initial) and date each engagement working paper.
- Each engagement working paper should contain an index or reference number.
- Audit verification symbols (tick marks) should be explained.
- Sources of data should be clearly identified.

THE ESSENTIAL ELEMENTS OF A WORKING PAPER

- Decide on a standard format and design a template of this format.
- Neatness
- Clarity of meaning
- Make full use of the working papers developed in previous and other audits related to the same institution, for example, flowcharts, system descriptions and other data may still be valid.

Topic 7: Reporting and follow-up on the completion of audit assignment

List the characteristics of good internal audit reporting.

- Only important matters should be reported.
- Internal audit reports should be useful and timely.
- Internal audit reports should be accurate and adequately supported.
- The findings should prompt the management to take action.
- Audit reports should be objective and should contain sufficient information.
- Internal audit reports should be clearly and simple presented.
- Internal audit reports should be concise.
- Internal audit reports should have a constructive impact.
- Internal audit reports should be logically arranged and positive.

Writing Internal audit reports

- The internal auditor should give an overall opinion and report that a manager is either
  - meeting the standard or
  - not meeting the standard
- The basic objectives of internal audit reports are:
  - to supply useful and timely information on operational deficiencies and other aspects and
  - to suggest improvements in the way in which the organisation is run
- The internal audit report therefore serves a twofold purpose, namely
  - to communicate the results of an internal audit
  - 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

Additional Assurance engagement communication standards

The standards offer guidance regarding:
the quality of assurance engagement communication
what is required in the event of an error or omission

Quality of communications

- **Accurate** – communication is free from errors and distortions and are faithful to the underlying facts
- **Objective** – communications are fair, impartial and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances
- **Clear** – communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.
- **Concise** – communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy and wordiness
- **Constructive** – communications are helpful to the engagement client and the organisation and lead to improvement where needed.
- **Complete** – communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions
- **Timely** – communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Perform observation evaluation and escalation process

The internal auditor must asses each observation using an evaluation and escalation process
Evaluate factors affecting the observation relative to its impact, likelihood, classification and the way in which it affects the mitigation of risk
See Fig 14.4

Elements of an audit finding:

Observations and recommendations are based on the following criteria:

- Criteria/standards – the standards, measures or expectations used in making an evaluation and or verification
  - 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?
- Statement of condition – the factual evidence that the internal auditor found in the course of the examination (the current state)
  - What was found?
  - What was observed?
  - What is not functioning effectively or efficiently and what is defective?
  - Is the condition isolated or widespread?
- Cause – the reason for the difference between expected and actual conditions
  - Why did it happen?
  - What was the underlying cause of the deviation?
  - What caused the activities to become inefficient and uneconomic?
- Effect – the risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria.
  - What is the significance?
  - What is the consequence of the finding?
  - What will the final result be if the condition continues?
- Recommendations – suggested corrective actions to correct the condition
  - What could be done to rectify the situation?
  - What recommendations are practicable and reasonably acceptable?
  - Who should implement the recommendations?

Basic characteristics of good internal audit reporting:

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

The format of internal audit reports

- management summary (if applicable)
- background
- overview
- opinion/general evaluation
- findings, recommendations and conclusions
- comments by the auditee

Presenting internal audit reports

- Promoting two-way communication and feedback
- Communicating an urgency and immediacy to the subject
- Enhancing the internal auditor's flexibility
- Enhancing the internal auditor's credibility
- Facilitating group ownership and commitment

The presenting process

- preparing the outline
  - who the recipients are
  - what message is to be communicated
  - what action the internal auditor wants the recipient to take
- structuring the outline
  - It reduces anxiety as the internal auditor knows what is going to be said next and where key points are going to be stressed.
  - It ensures the presentation is management-oriented.
  - It helps the internal auditor to present his findings and opinion logically.
  - It enables the managers to follow easily.
  - It provides a framework to fall back on if the discussion moves away from the original purpose.
- preparing the draft presentation
  - Have I considered managers' needs?
  - What benefits and values are there for the managers?
  - What are the facts?
  - Is the intended message coming through?
  - Am I being honest
- editing the draft presentation
- selecting the presentation method