Domain 1: The Information System Audit Process

Organization of the IS AUDIT function

How will you establish the role of the IS audit function؟

The role of the audit function is described in the Audit Charter.

What are the five (5) components of the Audit Charter؟

1. Scope of the audit
2. Responsibility of the audit function
3. Management’s responsibility
4. Objective and delegation
5. Delegation of authority

Who approves the Audit Charter؟

Senior management or the top-level management

IS Resource Management

How should an audit begin؟

1. Audit charter
2. Project plan for the audit
3. Availability of the proper skills

What if the proper skills are not available for the audit? Is it acceptable to ask the auditee to help؟

Auditors should obtain the appropriate skills. If the auditee provides help during the auditing process, the audit might not be very objective, so it should be avoided.

Audit Planning

What are the two (2) types of Audit Planning؟

1. Short term (less than a year(
2. Long term (more than a year(

How often should the Audit Planning be reviewed؟

At least once a year.

What are the five (5) factors that should be considered in an Audit Plan؟

1. Risk assessment
2. Local and international regulatory requirements
3. Corporate deadlines
4. Future technologies
5. Limitation of information subsystems

What five (5) step strategy should an IS Auditor use to draw up an Audit Plan؟

1. In-depth understanding of the business and its
   a. Mission statement
   b. Business objective
   c. Process involved
   d. Technology
2. Risk assessment
3. Internal control
4. Setting the scope and objective of the audit
5. Development of the audit strategy.

What are the six (6) common methods the auditor can use to understand the auditee’s business؟

1. Acquire domain knowledge
2. Annual reports, reading on web, industry publications

3. Review the short-term and long-term plans
4. Meet the key managers
5. Review the previous audit reports
6. Tour the organization

What is the biggest challenge for the IS auditor in terms of planning the audit؟

Matching the available resources with the audit plan.

Effect of laws and regulations on the Audit Plan

What are the four (4) common types of laws and regulations an IS auditor should know about the auditee's business؟

1. Federal law regarding the business
2. State law applicable (if any(
3. Industry-specific law; for example, banking industry has its own set of rules and regulation
4. International law (where applicable(

ISACA IS Auditing Standards

What are the objectives of the ISACA IS auditing standards؟

1. Minimum level of acceptable performance, as per the Code of Professional Ethics
2. Should meet the professional's expectations.

Risk, Risk Analysis and Risk Management

What is risk؟

Risk: The possibility of something harmful or damaging occurring is known as risk. In technical terms, risk is the probability of a threat or a threatening agent exploiting the system's vulnerability.

The ISO’s guidelines for the Management of IT Security defines risk as:

"The potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat".

What is a Business Risk؟

This is a risk that may have an impact on the following:

1. Asset
2. Process
3. Objective of organization or business

What is Risk Management؟

Risk Management: The process of identifying, assessing and minimizing the risk to an acceptable level and, later, maintaining that level.

What is the primary role of Risk Management؟

1. To identify the threat
2. To estimate how often threats occur

What steps are required in a typical Risk Management project؟

1. Identify the business objectives
2. Carry out a Risk Analysis (quantitative or qualitative), which has three components:
    i. Asset-related: (includes hardware, software, processes and any resource valuable to the organization(
        1. Asset identification
        2. Valuation of asset

    ii. Threat
        1. Identification of threat
        2. Probability determination of each threat

    iii. Vulnerability
        1. Likelihood and/or
        2. Probability of occurrence
3. Assess the risk
4. Risk Control and Treatment: avoidance or mitigation with the help of
    i. Safeguards

    ii. Counter-measures
5. Delegate or accept risk

Important Note:

In the classical methodology, first the critical assets are identified and then the threats. However, some organizations start with identifying the threats rather than the assets, which is perfectly acceptable.

How can an event that may result in loss be identified؟

1. Actual threat
2. Threat probability
3. Threat has already materialized and the organization is facing the consequences.

What is the nature of the threat؟

It can be one of the following:

1. Financial
2. Regulatory
3. Operational

What are the four (4) basic questions that should be asked during the Risk Analysis؟

1. What is the value of the asset؟
2. What is the threat؟
3. What are the vulnerabilities؟
4. What is the likelihood of occurrence؟

What are the two (2) main purposes of the Risk Assessment؟

1. Quantifying the impact of the threat
2. Putting a price tag or price value on the risk or the impact on the business

What is the end result of the Risk Assessment؟

1. Identification of the risk
2. Recommendations regarding safeguards and countermeasures with cost/benefit justifications

What is the difference between Risk Assessment and Risk Analysis؟

Sometimes the terms are used interchangeably; however, when they are differentiated, it is on the following terms:

Risk Analysis	Risk Assessment
Initial stage	More advanced stage
Initial step	In a way, a Risk Analysis is the prerequisite for a Risk Assessment
The identification of assets, related threats, VA and probability of occurrence	Once the threat is identified, Risk Assessment deals with quantifying the

	impact and putting a price tag on the risk.

What is the Risk Management Triple؟

1. Asset
2. Vulnerability
3. Threat

What are the four (4) key components of Risk Assessment؟

1. Asset
2. Vulnerability
3. Threat
4. Safeguards

What types of items are included as assets؟

1. Products
2. Resources
3. Processes

How is an asset valued؟

An asset is valued on the basis of:

1. Cost incurred in terms of
    a. Creation
    b. Development
    c. Support
2. Plus the cost when it is
    a. Replaced
    b. Refurbished/overhauled
3. Plus the actual market cost
4. Plus the goodwill cost

What is a Threat؟

A threat is an event that might cause harm or have an undesirable impact on the system. A threat can be natural or man-made.

What is a Vulnerability (VA؟ (

A vulnerability can be defined as a security loophole or an open door. It is basically a weakness in the system, or in the infrastructure. Threats exploit vulnerabilities.

What is a Safeguard؟

A safeguard is also known as a "counter-measure". The main objective of a safeguard or counter-measure is to overcome the threat, resulting in the reduction of risk.

Rule of Thumb: If you are confused as to whether something is a threat or a vulnerability, put yourself in the situation. For Example: You can say to yourself, “ I can be threat to an organization but vulnerability, I can’t”.

What is an Exposure Factor؟

The Exposure Factor (EF) provides the percentage of loss if a certain adverse event takes place. Take the case of an electrical surge in the power supply to a key component, for example. If the component burns out, this might represent 25% of the entire exposure. The EF will then be .25%

What is an ARO؟

ARO is the Annual Rate of Occurrence.

1. It is an estimation of the frequency of a threat occurrence in a year.
2. If a hard disk crash occurs once in five years, the ARO will be 1/5 = ..20
3. The ARO can be a whole number or a fraction.

What is an ALE؟

ALE is the Annual Loss Expectancy, representing the loss in terms of the dollar value.

What are the key equations for Risk Assessment؟

Single Loss Exposure ($) = Asset Value ($) x Exposure Factor (%)

Annual Rate of Occurrence = Number of occurrences ÷ Number of years

Annual Loss Expectancy ($) = SLE ($) x ARO

How is the value of the ALE useful to the organization؟

If the ALE is $5000 and the safeguard cost is $100,000 over five years, the per year safeguard cost will be 100,000/5 = $20,000/year.

It is obviously not feasible to spend $20,000/per year for an Annual Loss Expectancy of .5000$

Points to remember:

1. The value of all assets should be known
2. The auditor should be aware of the Exposure Factor (EF) percentage.
3. Management concerns itself only with the ALE
4. The EF is always given as a percentage
5. The EF provides the possible degree of destruction to an asset
6. The EF represents the percentage of loss, not the percentage chance of occurrence
7. The EF is the percentage of loss, irrespective of the frequency of occurrence. It might occur once in three years or three times in one year.

What is the Quantitative Risk Assessment؟

1. Measurement of the potential loss (EF and SLE(
2. Establish rate of occurrence (ARO(
3. Calculate value (ALE(

How do is a Qualitative Risk Assessment Analysis performed؟

1. No hard and fast rule
2. Scenario-oriented
3. Based on the same assets and threat scenarios as in the Quantitative Analysis

What is the role of the Delphi Technique in Qualitative Risk Analysis؟

The Delphi Technique is simply a group discussion method, where each member has a vote.

1. Group members are asked to write down their responses
2. All responses are compiled and distributed to members
3. Their comments are written down, and are again compiled and redistributed
4. The process continues until consensus is reached

How do the Quantitative and Qualitative Risk Assessments compare؟

Quantitative	Qualitative
Objective	Subjective
Dollar value is assigned to risk	No dollar value is assigned
Cost Benefit Analyses	No
Automated (how?) and complex	No automation; less complex
Less guess work	More guess work
Result easy to communicate	Result difficult to communicate

What is a PSE؟

PSE stands for Preliminary Security Examination. Top management reviews the PSE prior to launching a Risk Assessment assignment.

What are the components of a PSE؟

1. Asset cost/value
2. Listing of threats

.3 Documentation of existing security measures.

What is the difference between a Risk Analysis and BIA؟

Risk Analysis	Business Impact Analysis
More complex	Less complex
Most companies need to perform a Risk Analysis exercise when they start out	Undertaken once the Risk Analysis has been performed. Later, if small magnitude changes are needed, a BIA is performed.
-3Step Process	Same 3-Step Process

In technical terms, what are the three steps of a Risk Analysis؟

1. Estimate possible losses
2. Analyze the threat
3. Define ALE

How is the Risk Analysis carried out؟

The Risk Analysis is carried out by a simple three-step process:

<u>Step 1:</u> Estimate Potential Losses

a. Valuation of the Asset
b. Calculation of SLE

<u>Step 2</u>: Analyze the threat potential

a. Probability of threat occurring
b. Find the asset VA
c. Estimate ARO

<u>Step 3</u>: Calculate ALE

a. ALE = SLE x ARO

What is the checklist of threat sources؟

1. Internal users
2. Hackers
3. International or regional conflict
4. Badly-defined Operational Procedures
5. Poorly written applications
6. Environmental hazards
7. Weak computer infrastructure
8. Misplaced priorities

What is the checklist for compiling the Risk Analysis؟

1. List of critical assets
2. Critical asset costs
3. List of threats
4. Probability that threat will occur
5. Potential losses
6. Remedial measures

How do you estimate Potential Losses؟

1. Valuation of assets
2. Calculate SLE

Once the risk is defined, how it is handled؟

1. **Risk Reduced:** With the help of safeguards
2. **Risk Transferred:** With the help of insurance and other instruments
3. **Risk Accepted:** Management is aware of the risk, but there are not sufficient funds available to reduce or transfer the risk
4. **Risk Rejected:** Management does not accept the risk in the first place

What is the most difficult part of Risk Assessment؟

Asset Valuation is the most difficult part of RA.

How is the Asset Valuation carried out؟

1. Take the initial cost
2. Establish the cost of testing
3. Estimate the cost of roll-out
4. Estimate the cost of maintenance
5. Lastly, establish the value in the open market (external to the company(

Why is Asset Valuation so important؟

Asset valuation is a prerequisite for the following activities:

1. Risk Assessment
2. Business Impact Analysis
3. Selecting the correct safeguard
4. Cost Benefit Analysis
5. Security audit
6. Security control

What happens if the Information Asset Valuation is not done properly؟

This could result in the following:

1. Improper controls
2. Protection of the incorrect assets
3. Acquisition of the wrong safeguard

What is a prerequisite for applying the security controls؟

You must define the value of the information.

What is Risk Mitigation؟

1. Selecting a counter-measure / safeguard
2. Accepting the residual risk
3. Implementation of control and monitoring mechanisms

What is the Total Risk؟

Total Risk = Threat x Vulnerability x Asset Value

What is the Residual Risk؟

It is a well-known fact that it is impossible to ensure 100% security. If you have implemented safeguards against 95% of threats, then the Residual Risk is .5%

Residual Risk = Total Risk - Safeguards

Safeguards:

What is the next step, once the Risk Assessment has been completed؟

Search for the counter-measures and safeguards

How are safeguards selected؟

The threats are matched against the appropriate safeguards.

What to look for when selecting a safeguard:

1. Functionality
2. Cost
3. Cost Benefit

What is the most important factor to be considered before a safeguard is implemented؟

A Cost Benefit Analysis is essential before a safeguard is implemented.

What should be the default of a safeguard؟

The default should be a fail-safe, with the fewest possible privileges

Selection of Safeguards

On what basis are safeguards selected؟

The safeguard selection criteria can be divided into two categories:

I. Primary Criteria

i. Cost/Benefit

a. ALE before safeguard	US$ 20,000
b. ALE after safeguard	2,000
c. Reduction in ALE (a-b(	18,000
d. Cost of safeguard per year	5,000
e. Benefit from safeguard (c-d(	13,000

ii. Minimal Manual Intervention

a. Operations should be simple

b. Most operations should be automated

iii. Recovery from Failure

a. Recovery should be safe

b. No asset destruction

c. No rights violation

II. Secondary Criteria

i. Easy to Audit

a. Must provide an audit of logs

b. Viewer for log is preferred

ii. Vendor Support

a. Local vendor or local support

b. Proven solution

iii. Easy to Maintain

a. Average person should be able to maintain it with formal training

b. Simple operations and troubleshooting

Risk Analysis and Auditing

Why is risk analysis part of Audit Planning?

A risk analysis helps to identify the following:

1. Risk
2. Vulnerability

Once the risk and vulnerability have been defined, it is easier for the auditor to determine the controls.

Internal Controls

What is the purpose of using internal controls?

Internal controls provide the following:

1. Assurance that the organization’s objectives are met
2. Prevention or mitigation of risk of undesired events

What are some examples of internal controls?

1. Policies
2. Standards
3. Procedures and Practices.

What is the relationship between control and the control objectives?

Control is way in which the control objectives are met.

Who has the ultimate responsibility for the control?

Senior Management

How is the strength of the control measured؟

The strength of the control is measured in the following terms:

1. Design strength
2. Effectiveness

When evaluating the strength of the controls, what factors should be considered؟

1. Preventive or detective
2. Formal or ad hoc
3. Manual or Automated/Programmed

Internal Control Objective

What is an Internal Control Objective؟

This is a statement used to implement a particular "control procedure” for a certain activity.
Or
A statement of the desired result achieved by implementing certain control procedures for a particular activity.

What are the main objectives of implementing internal control؟

1. Protecting and safeguarding the asset
2. Assuring integrity for the resources
3. Ensuring effectiveness and efficiency of the options
4. Complying with growth polices and procedures
5. Providing business continuity and disaster recovery capability.

What are the three (3) major controls in the Internal Control System؟

1. Internal accounting control: Related to the accounting function.
2. Operational controls: Related to day-to-day operations
3. Administrative controls: Compliance with management polices and operation efficiency in the functional areas. (Administrative controls also support the operational controls, to some extent(

What are some examples of Information System Control objectives؟

To ensure:

1. Information is up-to-date and secure
2. Data entered in the system is relevant
3. All of the rejected logins are reported
4. Duplicate records are recorded and reported for securitization
5. Data is backed up
6. Changes follow the change control procedures

Information Systems Control Procedures

What do the control procedures include؟

1. Policies
2. Practices

What are some examples of control procedures؟

1. Strategy and direction
2. System administration and change control management
3. Data processing controls
4. Quality Assurance procedures
5. Physical controls
6. DRP/BCP
7. Database administration controls.

What is the relationship between General Control Procures and IS-Specific procedures؟

Normally general control procedures can be mapped to Information System procedures

What are the six Information Control procedures؟

1. General organization control procedures
2. Control of access to data and programs
3. System development controls
4. Data processing operations
5. Technical support controls
6. Processing of Quality Assurance control

Does the “Internal Control Objective” apply only to the manual system؟

No; it applies to all areas, manual or automated. However, the control implementation features are different.

COBIT

What is COBIT؟

COBIT stands for the Control Objectives for Information and related Technology.

What does COBIT provide؟

1. Framework for Information System control
2. Good practices for IT governance
3. Control and assurance for effective use of IT

How many hi-Level and detail control objectives are there in COBIT؟

Hi-level objectives: 34

Detail objectives: 300 plus

How many standards does COBIT relate to؟

36plus.

What are the six (6) components of COBIT؟

1. Executive Summary
2. Framework
3. Control objectives
4. Management guidelines
5. Audit guidelines
6. Implementation toolset

What are the three major classifications of controls؟

1. Preventive
2. Detective
3. Corrective

What are some examples of preventative controls؟

1. Employing well-qualified people
2. Segregating duties
3. Well-designed documents
4. Implementing proper procedures
5. Edit Checks
6. Controlling access

What are some examples of detective controls؟

1. Hash Totals
2. Check points
3. Error Message
4. Performance Review
5. Double checking of calculations

What are the examples of corrective controls؟

1. Recovery Procedures
2. Disaster Recovery Planning

Performing an Information System Audit

What is Auditing؟

A structured process by which an independent, competent person obtains relevant evidence to ascertain an opinion regarding an event or economic entity, and reports conformance to a pre-defined set of standards.

What does the audit program consist of؟

1. Objectives
2. Audit Procedures

What is required from an IS auditor during the audit process؟

1. Ascertain the objectives
2. Gather evidence
3. Evaluate the control strength
4. Prepare the report
5. Present to management

What are the five (5) types of audits؟

1. **Financial Audit**: Focuses on the integrity and reliability of the financial statement
2. **Operational Audit:** Evaluates the internal controls of a given area
3. **Integrated Audit:** Financial audit + Operational audit
4. **Administrative Audit**: Evaluates the efficiency of an organization's operational activity
5. **Information Systems Audit**: Evaluates Information Systems and related resources. The main emphasis is on the following:
    a. Safety of assets
    b. Integrity of data
    c. Confidentiality of information
    d. Presence of appropriate internal controls

What is the major difference between an IS audit and other types of audit؟

As all audits are based on objectives and scopes, the IS auditor sees things from a different aspect , such as confidentiality, availability, quality, efficiency, service and reliability.

What are the "General Audit Procedures" in a typical audit؟

1. Understanding of the audit area
2. Risk assessment and audit schedule and plan
3. Preliminary review
4. Evaluations
5. Control test
6. Further testing, i.e. substantive testing
7. Communication of result and preparation of report
8. Follow-up

What should the IS auditor be aware of regarding the testing and evaluation of the Information System control؟

1. Third party generalized audit software used to survey contents, e.g. the data file
2. Flow-charging technique
3. Specialized software used at the Operating System level in order to understand vulnerabilities.
4. Use of previous audit report

Audit Methodology

What is the Audit Strategy or Methodology؟

This is a set of audit procedures (documented) used to achieve the audit objective.

What are the components of an Audit Strategy؟

1. SOS (Statement of Scope(
2. Statement of Audit Objectives
3. Statement of Work Program

What are the eight (8) steps in a typical audit؟

1. Identify the area to be audited.
2. Audit Objective
3. Audit Scope
4. Pre-Audit Planning
5. Data-gathering and audit procedure
6. Review the result
7. Methods of communications to communicate result to the senior management
8. Audit report

What is the difference between an Audit Objective and an Audit Scope؟

Audit Objective: Purpose of audit, e.g. in e-banking, whether proper controls are there or not.

Audit Scope: Specify the function, system or unit to the included in audit

What are the two major components needed in pre-audit planning؟

1. Identification of technical skills
2. Resources needed.

What sources of Information can be used in the pre-audit planning phase, in order to get a better understanding of the auditee؟

1. Polices and procedures
2. Standards and guidelines
3. Previous audit work

What information is included in a typical audit report؟

1. Follow-up procedure of the last audit
2. Process to evaluate
3. Procedure to test the controls
4. Evaluations of policies, procedures and documentation

What is the Audit Program؟

It is a product of the audit process.

What does the Audit Program provide؟

1. Guide for recording and documenting the steps of the audit
2. Type and extent of the matter reviewed
3. Accountability of the performance

Audit Risk and Materiality

What is the new trend in the auditing approach؟

Risk-based auditing

What are the different tests in risk-based auditing؟

Auditor to decide between two types of testing, i.e.

1. Compliance Testing or
2. Substantive Testing

What are the five steps in risk-based auditing؟

1. Gather the information and do the planning
2. Understand the internal controls
3. Perform the compliance test
4. Perform the substantive test
5. Write the reports and recommendations

How can the IS auditor gather information؟

1. Review the business's and industry's products
2. Previous year's audit report
3. Financial information
4. Web site of the company
5. Web site of the competition

How can the internal control be understood؟

The internal control can be understood through an examination of the control environment, carrying out a Risk Assessment, control procedures, etc.

What does the compliance test evaluate؟

Mainly it tests the policies, procedures and segregation of duties.

What is a substantive test؟

This is a detailed test.

What is the audit risk؟

This refers to the risk of having an incorrect assumption about the subject under audit.

What is the material risk؟

This term refers to errors or non-compliance or a weakness in the internal control, which can be a significant threat to the organization.

How can a threat be identified as “significant” or not؟

Through the use of a risk-based audit report.

Is the significance of non-compliance absolute or relative؟

It is relative. Something that is significant at the operations level might not be significant for top management.

How can audit risk be avoided؟

If the sample is chosen “scientifically”, the audit risk is minimized.

What role do “inherent risk” in detection risk or “control risk” in “risk-based auditing” play؟

They play no role; they are not assessed.

On what bases do IS auditors rely؟

IS auditors rely on the risks inherent in

1. Internal Control
2. External Controls

What are the three (3) areas of business risk؟

1. Financial
2. Regulatory
3. Operations

Why is it necessary for IS auditors to understand the nature of the business؟

If the IS auditor understands the business, he is in a better position to identify the risk and categorize it accordingly.

What is a Risk Model Assessment؟

This specifies the weights for the different types of risks associated with a particular business.

Risk Assessment Techniques

Which business should be audited first؟

A business with high risk.

How are the high-risk areas determined؟

Through the use of a risk Assessment.

How does the risk assessment help to determine which areas should be audited؟

1. Limited auditing resources are effectively allocated for high-risk area auditing
2. A Risk Assessment helps the auditor focus on the relevant critical business information for top management
3. Improves efficiency

What are the different methods for carrying out Risk Assessments؟

1. Scoring System
2. Judgmental

What does the scoring system do؟

The scoring system makes use of the risk factor to prioritize the audits.

What variables are considered in the scoring system؟

1. Technical Complexity
2. Financial loss (if any(
3. Level of control procedures

Are the variable always weighted؟

No, these are not always weighted.

How do scoring systems help in auditing؟

Audits are scheduled for those areas with higher risk values.

With regard to selecting the area to be audited, what is the judgmental method؟

When the judgmental method is used, decisions are made based on following:

1. Business insight
2. Senior management directives
3. Business goals
4. Results of earlier audit

Will the risk assessment methods remain the same in the future؟

No, the methods might change based on the needs of the organization.

Audit Objectives

What is the difference between Control Objectives and Audit Objectives⸮

Control Objectives	Audit Objective
Focus is on the functioning of the internal control.	Focus is on the "specific goals" that the audit should achieve

With regard to access, what should the audit include⸮

1. Compliance with regulatory and legal requirements
2. Assessment of the confidentiality, integrity and availability of information.

Is it possible that management will give the IS Auditor some General objectives⸮

Yes, the IS auditor may be given some general objectives. For example, the auditor might be asked to:

1. Audit the internal control of application development
2. Audit the integrity of the core business application.

What is the key element in planning the Information System audit⸮

It is the mapping, or the translation of:
Basic audit objectives ➦ Information System objectives.

So, the IS auditor should have the skills to understand that the basic objective of an audit can be mapped to the IS control objectives.

What is the basic purpose of an IS Audit⸮

1. Identify control objectives
2. Establish Related controls for addressing objectives

What should the IS auditor identify in the initial review؟

Firstly the IS auditor should identify the initial controls.

What does the IS auditor specify in the initial review؟

The key controls

How are the controls tested؟

Through the use of the following:

1. Compliance
2. Substantive Testing

What is the difference between Compliance and Substantive Testing؟

Compliance Testing	Substantive Testing
The compliance testing is done initially to check whether the key controls are working	Substantive testing usually follows compliance testing
Testing of the control (for compliance(	Testing of integrity
Check compliance against policies and procedures	Used for monetary transactions or places where there is little structure.
Mostly dependent on the availability of trail documentation	Not very dependent on the documentation.
Once the documentation is available for a particular issue, the compliance test is positive	Availability of documentation is not enough. The validity and integrity of the documentation are challenged in the testing

What is the correlation between the level of internal control and the amount of substantive testing required؟

1. The more adequate the controls, the fewer substantive tests are needed.
2. The weaker the Internal Control, the more substantive tests are needed.

What are the four (4) steps for checking control in an environment؟

1. **Preview:** The system is previewed so that the controls can be checked
2. **Compliance test:** Confirms the functionality of the controls
3. **Control evaluation:** Evaluates the scope and size of the substantive test
4. **Substantive test:** Evaluates the validity of the data

What are the two (2) types of substantive test؟

1. Test for balances and transactions (more financially related(
2. Test for analytical procedure review

Evidence

What is the definition of evidence؟

This is proof, in the form of information or documents, that the organization is following certain audit criteria or objectives.

What is the importance of evidence؟

The auditor's opinion is based on the evidence gathered.

What are the five (5) forms of evidence that the IS Auditor can use؟

1. Auditor observation
2. Interview notes
3. Correspondence extracts
4. Internal documentation
5. Results of the audit tests

What are the three (3) factors showing the reliability of the evidence؟

1. Provider of the evidence must be **independent.**
2. Provider of the evidence is **qualified.**
3. Evidence is more of an **objective** nature rather than subjective.

Should the IS auditor only look for "good evidence؟ "

No, the auditor should focus on evidence that supports the objective, not on whether the evidence is good or bad.

How does the quality and quantity of the evidence map to IFAC (International Federation of Accountants؟ (

ISACA	IFAC
Quality of the evidence	Competency, i.e. validity and relevancy
Quantity of the evidence	Sufficient – The auditor decides whether the evidence is sufficient

What is ISCA number stands for auditing؟

060.020

What techniques are used to gather evidence؟

1. Review of IS Organization Structure
2. Review of policies, standards and procedures
3. Baseline documentation for
    a. Input validity
    b. Information processing
    c. Integrity of the process
    d. Validity of the output
    e. SDLC DOCUMENTATION
    f. User manual
    g. Operation manual
    h. Log files
    i. Quality Assurance Reports

Is traditional documentation required for CASE or prototyping؟

No, traditional documentation is only required for SDLC and related methodology, but not for CASE and prototyping.

What documentation is relevant for CASE and prototyping؟

1. Initial requirement and justification of the project
2. Database specification
3. File layout and others.

Sampling

When is sampling used؟

Sampling is used when time and cost are the constraints and verification of the total policy is not possible.

What is the meaning of population with respect to sampling؟

Population refers to all the members of a group which need to be examined.

What is a sample؟

A sample is the subset of the population.

What is a sample used for؟

Often it is used to draw an inference about the characteristics of the population.

Sampling Basics - Confidence Coefficient & Level of Risk

What is the confidence coefficient؟

The confidence coefficient is the probability that the sample is truly representative of the population.

How is the confidence coefficient represented؟

It is represented as a percentage.

At what confidence coefficient level should the IS auditor feel comfortable؟

%95

What is the relationship between the confidence coefficient and sample size؟

The higher the confidence coefficient, the greater the sample size. For greater confidence a bigger sample size is needed; e.g., if the confidence coefficient is 100% (which it can't be), 100% of the population would have to be used.

What is the difference between the "Confidence Coefficient", "Confidence Level" and "Reliability Factor؟ "

No difference; they all refer to the same thing.

What is the level of risk؟

Level of Risk = 1 - Confidence Coefficient

Sampling Basics - Precision

What does the term ‘sampling precision’ refer to؟

Precision is the acceptable range of difference between the actual population and the sample.

What is the difference between Precision and Confidence Level؟

1. Precision is the opposite of Confidence Level
2. When the precision level is low, the confidence level is high

Which is better: a higher or lower precision level؟

1. If the required precision is 0%, this means that there would is no difference between my sample and the population, i.e. Sample Size = Population. Even with a precision of 5%, the sample is almost as big as the population.
2. Similarly, if the precision is 100%, this means that Actual - Sample = 100% difference is acceptable
3. The precision level should be decided by the IS Auditor.

What is the relationship between Precision and Sample Size؟

The relationship is inversely proportional.

What is the difference between "Attribute Sampling" and “Variable Sampling؟ ”

Attribute Sampling: Represented as a percentage

Variable Sampling: Represented in numbers, or the monetary amount.

What is the difference between "Precision range” and "Precision Mean؟ "

There is no difference; they mean the same thing. (Substantive testing(.

Sampling Basics - Expected Error Rate & Tolerable Error Rate

What is the Expected Error Rate (EER؟ (

As the name indicates, this refers to the expected errors, represented as a percentage of the error.

What is the effect of EER on Sample Size؟

It is directly proportional, i.e. if the EER is high it means that more errors are foreseen. Smaller the sample size, there is possibility of bigger EER.

How is the EER applied to the variable sampling formula؟

The EER is not applied to the variable sampling formula; it is only used with the "Attribute Sampling" formulas.

What is the tolerable error rate؟

This is the number of errors or mis-statements that can exist without the result being materially mis-stated.

How are tolerable error rates used in sampling؟

They are used to plan the upper limit of the "precision range" for testing compliance.

How is the tolerable error rate represented؟

It is represented as a percentage.

Sampling Basics - Standard Deviation and Variance

What is the prerequisite of Standard Deviation؟

The sample mean.

What is the sample mean؟

Sample Mean = Sum of Sample Value/ Sample Size

The mean of a random sample is an unbiased estimate of the mean of the population from which it was drawn.

Another way to say this is to assert that regardless of the size of the population and the size of the random sample, it can be shown (through the Central Limit Theorem) that if random samples of the same size were repeatedly taken from the same population, the sample means would cluster around the exact value of the population mean.

What does the sample mean indicate؟

The average size of the sample.

What is Standard Deviation؟

To calculate the standard deviation of a population it is first necessary to calculate that population's variance. Numerically, the standard deviation is the square root of the variance. Unlike the variance, which is a somewhat abstract measure of variability, the standard deviation can be readily conceptualized as a distance along the scale of measurement.

What is Variance؟

Variance calculates variability that characterizes the dispersion among the measures in a population. Numerically, the variance is the average of the squared deviations from the mean.

To calculate the variance of a given population:

1. First calculate the mean of the scores
2. Measure how much each score deviates from the mean

.3Square that deviation (by multiplying it by itself .(

What is the Standard Deviation؟

Standard deviation is the square root of the variance.

What is the Sample Standard Deviation؟

This refers to the variance of the sample from the sample mean.

What is the Population Standard Deviation؟

Measures the deviation from the Normal Distribution.

What is the relationship between the standard deviation and sample size؟

The relationship is directly proportional. As with any of the error measurement tools, the higher the standard deviation or EER, the larger the error / deviation can be expected. In order to minimize these effects, the sample size must be increased.

How can a population’s standard deviation be applied to the attribute sampling formula؟

It can’t; it can be only applied to the "Variable Sampling Formula."

Other Sampling Issues

What are the two approaches for auditing؟

1. Statistical Sampling
2. Non-Statistical Sampling (also known as Judgmental Sampling(

What is the difference between Statistical Sampling and Non-Statistical Sampling؟

Statistical Sampling	Non Statistical Sampling
Objective in nature. Used for determining the following: a. Sample Size b. Selection Criteria	Subjective; uses auditor's judgment to determine the following: a. Sample Size b. Selection Criteria
Quantitative decision	Qualitative decision
Quantifiable result	Non-quantifiable result

In statistical sampling, how can the closeness of "sample size" be determined؟

The closeness is represented by the sample's precision

How does one know that the sample is reliable؟

The reliability or the confidence level is presented by a number between 1 and .100

How is the final assessment represented in Statistical Sampling؟

It is represented as a percentage.

What is Sample Risk؟

Sample size is not a true representative of the population and the conclusion drawn from the sample is wrong.

What is the "confidence coefficient؟ "

This quantifies the probability of error in the sample.

What is the ideal statistical sample؟

Each item in the population should have an equal opportunity to be selected.

What are the two general approaches؟

1. Attribute Sampling
2. Variable Sampling

What are the differences between attribute sampling and variable sampling؟

Attribute Sampling	Variable Sampling
Used in compliance testing situations	More commonly used in substantive testing
Focuses on whether the attribute is present or absent	Focuses on the characteristics of the population e.g. weight, dollar, etc…
Output/conclusion is in the form of “Rate of Incidence”	Output/conclusion is in the form of “Deviation from the norm”
"Yes or No" check	Checks for “Yes, but also how much 'YES' has deviated from the normal

Attribute Sampling

What are the three different methods of proportional attribute sampling؟

1. Fixed sample-size attribute sampling
2. Discovery sampling
3. Stop-or-go sampling

What is the difference between “Attribute Sampling,” “Fixed Sample Size Attribute Sampling” and “Frequency-estimating Sampling؟ ”

None; they are all the same.

What are the main features of “Fixed Sample Size؟ ”

1. Look for the percentage of occurrence of attribute
2. Questions regarding “how many” questions are addressed

What are the features of “stop-or-go” sampling؟

1. Avoids excess sampling.
2. Useful when expected occurrences are low.

What are the features of Discovery Sampling؟

1. Used when the objective is to “discover” fraud or irregularities
2. Useful when expected occurrences of events are extremely low

Variable Sampling

What is the difference between “variable sampling”, “mean estimation sampling” and “dollar estimation؟ ”

There is no difference; they are all the same.

What is the variable sampling used for؟

To estimate the quantitative value, e.g. dollar, weight.

What are the seven (7) items the auditor should consider while evaluating the sample؟

1. Determine the test objective of the test
2. Define the populations
3. Determine the sampling method
4. Determine the sample size
5. Select the sample
6. Evaluate the sample
7. Confirm that the sample is representative of the population

CAAT

What is CAAT?

CAAT stands for Computer-Assisted Audit Technique. These are tools for auditors.

How can CAAT assist auditors?

CAAT assists the IS auditor in the following ways:

1. Access relevant data and information
2. Analyze the data as per the objective of the audit
3. Report findings.

Why is CAAT important for the IS auditor?

Today most of the evidence required by IS auditors is not in hard copy format; rather it is spread over different media across different platforms. The only way of collecting all these pieces of evidence efficiently is by using CAAT.

What are the five (5) Functional Capabilities of CAAT?

1. The ability to access files across different platforms
2. File manipulation and reorganization, e.g. indexing, sorting, linking and merging
3. Data selection on the basis of criteria and filtering conditions
4. Performs statistical functions, e.g. sampling, frequency analyses
5. Has an arithmetical function

What are some examples of CAAT software?

1. IDEA
2. ACL
3. SQL Command
4. Third party software
5. Other utility software

a. Database auditing software

b. Integrity testing software

What is GAS؟

GAS stands for Generalized Audit Software.

What are the sources of input for GAS؟

GAS can read and access the following:

1. Different databases
2. Flat files
3. ASCII files

What does GAS do؟

1. Collects data
2. Organizes information and sequencing
3. Mathematical computation
4. Stratification
5. Duplicate checks
6. Statistical analysis

What are the IS auditor’s concerns regarding CAAT؟

Prior to selecting the CAAT software, the IS auditor should check that it does the following:

1. Provides reliable results
2. Does not compromise the integrity of the system
3. Maintain the confidentiality of the client.

What does the CAAT program record and retain؟

1. Critical online reports
2. Comments on programs
3. Sample reports
4. Flow charts
5. File layouts
6. Recorded and filed definitions
7. Operating instructions

What types of accesses are recommended for the CAAT programs؟

Read-only access.

What are the limitations of CAAT؟

1. Might require more resources to install
2. IS auditor may need extensive training on the software
3. Integration with existing applications might be challenging.

Evaluating the Audit's Strengths and Weakness

What is the next step after the information and evidence for the audit have been gathered؟

Develop an auditing opinion.

What does the IS auditor do in order to develop an opinion؟

1. The auditor uses his/her experience
2. Assesses the results of the evidence.
3. With regard to compliance, he checks that the controls match the control objectives.

How should the control be evaluated؟

Controls should match the control objective and should minimize or remove risk or perceived risk.

How is the proper level of control assessed؟

Most of the time the Control Matrix is used for this.

How is the control Matrix constructed؟

1. Error types (top axis(
2. Control (side axis(
3. Matrix is filled using the ranking method
4. Once completed, the matrix shows the areas where the controls are lacking.

What are the compensating controls؟

A strong control in one area can compensate for a weak control in another area. This type of control is known as a compensating control.

What is the difference between a compensating control and an overlapping controls؟

1. A compensating control is when a strong control takes care of (supports) a weaker control
2. An overlapping control is when two strong controls cover the same area.

What should an auditor do regarding a compensating control and overlapping controls؟

Prior to reporting the control weakness, the auditor should see whether there are any compensating controls for the weak control area.

The auditor should report an overlapping control, as it might not be needed.

Materiality of the finding

What is the concept of the materiality of the finding؟

This refers to the decision whether to mention a particular finding in an audit report, based on its significance to the audience of the report. If the IS auditor concludes that the it is a "material error" and may lead to a larger problem regarding control, it should be reported.

To whom are IS auditors responsible؟

1. Senior management
2. The Audit Committee of the Board of Directors.

Why should the IS auditor discuss a matter with the management staff before communicating it to senior management؟

For two reasons:

1. Get consensus
2. Develop a corrective action plan

What is the end result of the IS audit work؟

An Audit Report.

What is the structure of the Audit Report؟

1. Introduction
    a. Audit Objective and Scope
    b. Audit Period Coverage
    c. Nature and Extent of the audit

.2 Auditor conclusion

.3 Auditor reservations

.4 Detailed findings and recommendations

Should the audit report only mention the negative points؟

No; the audit report should report both negative and positive (constructive) points.

Should the IS auditor insist that his/her recommendations be implemented immediately؟

No. Immediate implication might not be possible due to constraints in resources. However, the IS auditor can agree to planned implementation dates, and later the progress of the implementation should be monitored.

Should the IS Auditor mention some of his/her findings in the report, even if modifications are made prior to the report being given to the top management؟

Yes, the IS auditor should mention all of the findings, as they were at the start of the audit. However, he should mention that the issues are being addressed.

What should the auditor do prior to the releasing the reports؟

1. Discuss the recommendations
2. Establish the planned implementation dates/ time of implementation
3. Review and follow up on plans

What is the main sprit behind the audit؟

1. Presence of control based on the risk assessment
2. In the case where controls are missing, there should be some corrective action plan.
3. Once the report has been presented, there should be a follow-up to the corrective action

Do corrective actions resolve all of the problems؟

No, the corrective action may result in its own risks and problems.

What happens just prior to the end of the auditing assignment؟

An exit interview is conducted.

What is discussed in the Exit Interview؟

1. Findings and recommendations
2. Implementation dates
3. Justification of recommendations in terms of realistic approach and cost
4. Discussion of alternative and compensating controls

What is the IS audit documentation؟

This refers to the record and evidence of the audit work performed. It contains complete interview questionnaires, notes, system flowcharts, narratives and work papers.

CSA- Control Self-Assessment

What is the CSA؟

This is a formal method of examining the existing controls of the system in a professional way.

What are the two methods of self-assessment؟

1. Structured questionnaire
2. Automated tools

Is it possible to include outsiders in the CSA؟

Yes, if the skills are not available, it can be done.

What is the primary objective of an internal audit؟

To shift some of the responsibility from an internal audit to the functional areas.

Does a CSA replace the responsibility of the internal audit؟

No, it actually enhances it.

Who is responsible for the controls؟

Functional managers, e.g. the line managers.

What are the additional benefits of using a CSA؟

1. Education
2. Empowerment of the worker to assess the asset
3. Atmosphere to enhance the control environment

What are the three phases of a CSA؟

1. Planning
2. Implementation
3. Monitoring

What is the role of the auditor in a CSA؟

1. Assessment facilitator
2. Internal control specialist/professional
3. Leading and guiding the functional people to do a CSA.

How could an auditor understand the business before starting the audit؟

1. Preliminary survey
2. Walk-through

What is the first step in a CSA project؟

Conduct a meeting with the business unit manager to determine the scope and objective of the CSA.

What are the tools used in a CSA؟

1. Management meeting
2. Worksheet
3. Workshops
4. Questionnaire

What development techniques are needed for the CSA program؟

1. Information gathering
2. Empowerment
3. Decision-making.

What is the main advantage of a workshop-based CSA؟

1. Group decision-making
2. Empowerment of the employee.

How would you differentiate between the traditional approach and the CSA approach؟

Traditional Approach	CSA Approach
Primary responsibility is on the IS auditor	Primary responsibility is shared between the management and the IS auditor
Management and other staff are not directly responsible for the audit	Management and other staff are empowered to have more responsibility
Duties are assigned	Empowerment is carried out
Rule and policy-driven	Ongoing process of learning and improvement
IS auditor involvement is maximum. Employee participation is limited.	Employee participation is extensive. IS auditor involvement is limited.
Narrow focus	Broader focus
Only auditors and special consultants are involved	Staff members at different levels are involved.

Corporate Governance

What is corporate governance؟

This refers to the ethical corporate behavior of top management with regard to supervising, monitoring, controlling and directing the business entity, in order to safeguard the corporate assets and minimize the potential risk.

The Organization of Economic Co-operation and Development (OECD) defines it as:

"The distribution of rights and responsibilities among different participants in the corporation, such as the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set and the means of attaining those objectives and monitoring performance."

What are the advantages to proper corporate governance؟

1. A framework is formed to manage and report risk.
2. It is an internal method of monitoring, addressing and minimizing risk.