Information System Auditing Process I

Audit Planning

1. Which is the following best describes an audit universe?
   the list of all possible audits that could be performed within an organisation, covering all auditable areas.
2. Which of the following best describes a qualitative risk assessment?
   a risk assessment method that evaluates risk based on descriptive categories such as high, medium, or low.
3. Which of the following best describes a quantitative risk assessment?
   a method that uses mathematical models to calculate the probability and impact of risks in numerical terms.
4. Which of the following is the first step in risk-based audit planning?
   to identify high-risk processes in the company.
5. Which of the following is a major advantage of a risk-based approach to audit planning?
   optimum use of audit resources for high-risk processes.
6. Which of the following should be the first exercise while reviewing data center security?
   the evaluation of vulnerabilities and threats to the data center location.
7. Which of the following is the most important aspect of planning an audit?
   identifying high-risk processes.

Audit Charter

1. What is one of the primary benefits of having an audit charter?
   it defines the internal audit function’s role, enhancing its credibility and acceptance within the organisation.
2. Which of the following best describes the purpose of an audit charter?
   to establish the authority, responsibility, and accountability of the internal audit function.

3. An audit charter should be approved by
   Higher management
4. The audit charter should
   incorporate the scope, authority, and responsibility of the audit department.
5. The prime objective of an audit charter is to
   document the responsibility and authority of the audit department.
6. The document that delegates authority to the audit department is
   the audit charter
7. The prime reason for the review of an organisation chart is to
   understand the authority and responsibility of individuals.
8. An IS auditor would be primarily influenced by
   the charter of the audit department
9. Which of the following is the result of a risk management process?
   decisions regarding the security policy.
10. Which of the following should be included in an audit charter?
    the audit function's reporting structure.
11. The scope, authority, and responsibility of the IS audit function is defined by
    the approved audit charter
12. Which of the following functions is governed by the audit charter?
    the internal audit function.
13. Which of the following covers the overall authority to perform an IS audit?
    the approved audit charter
14. The audit function should be reported to the audit committee of the board because
    the audit function must be independent of the business function and should have direct access to the audit committee of the board.
15. The best objective for the creation of an audit charter is to
    provide the authority and responsibility of the audit function.
16. Main objective of an audit charter is to
    describes the auditors' authority to conduct audits.
17. Main objective of audit charter is to
    describe the auditors' right to access information.
18. Audit charter primarily includes

    the authority given to the audit function.

Electronic Data Interchange

1. Which of the following best describes a primary area of concern while auditing Electronic Data Interchange(EDI) based processes?
   lack of controls to ensure transaction integrity.
2. Which of the following is the area of greatest concern in an EDI process?
   the contract for a trading partner has not been entered.
3. Encryption helps in achieving which of the following objectives in an EDI environment?
   ensuring the confidentiality and integrity of transactions.
4. In an EDI environment, which of the following procedures ensures the completeness of an inbound transaction?
   the build segment count coming to the transaction set trailer of the sender.
5. In which of the following processes are details entered by one employee re-entered by another employee to check their accuracy?
   key verification
6. Which of the following is used in an e-commerce application to ensure that a transaction is enforceable?

   Non-repudiation

Internal Controls

1. Which of the following is the best example of a preventive control?
   implementing strong password policies to restrict unauthorized access.
2. Which of the following is the best of a detective control?
   using an intrusion detection system (IDS) to monitor network traffic.
3. Which of the following is the best example of a corrective control?
   running antivirus software to remove malware after it is detected.
4. Which of the following is the best example of a deterrent control?
   placing security cameras in visible locations to discourage theft.
5. Controls that are designed to prevent omissions, errors, or negative acts from occurring are which kind of controls?
   preventive controls
6. What are controls that are put in place to indicate or detect an error?
   detective controls

7. Which of the following is the segregation of duties an example of?
   preventive control
8. What is the process of using well-designed documentation to prevent errors an example of?
   preventive control
9. What kind of control is a control that enables a deficiency or another irregularity to be corrected before a loss occurs?
   corrective control
10. Utilizing a service of only qualified resource is an example of
    preventive control
11. A check subroutine that identifies an error and makes a correction before enabling the process to continue is an example of what kind of control?
    corrective control
12. Barriers or warning signs are examples of what kind of control?
    deterrent control
13. An "echo" message in a telecommunications protocol is an example of what kind of control?
    detective control
14. Checkpoints in a production job are examples of what kind of control?
    detective control
15. Controls that minimize the impact of a threat are what kind of controls?
    corrective controls
16. Controls that remedy problems observed by means of detective controls are what kind of controls?
    corrective controls
17. Controls that indirectly address a risk or address the absence of controls that would otherwise directly act upon that risk are what kind of controls?
    compensating controls
18. Controls that predict potential problems before their occurrence are what kind of controls?
    preventing controls
19. The requirement of biometric access for physical facilities is an example of what kind of control?
    preventive controls

20. Which of the following risks represents a process failure to detect a serious error?
    control risk
21. Which of the following statements best describes detective controls and corrective controls?
    detective controls are used to determine whether an error has occurred and corrective controls fix problems before losses occur.
22. Why are control objectives defined in an audit program?

    to give the auditor an overview for control testing.

Risk based Audit Planning

1. Which of the following best describes inherent risk?
   the risk of fraud or error occurring without considering any existing controls.
2. Which of the following best describes residual risk?
   the risk that remains after implementing security controls.
3. Which of the following is the most critical aspect in a risk analysis?
   identifying vulnerabilities.
4. What is the initial step in risk-focused audit planning?
   identifying high-risk processes.
5. What is the main objective of conducting a risk assessment?
   to ensure that critical vulnerabilities and threats are recognised.
6. What should be the next step of an IS auditor after identifying threats and vulnerabilities in a business process?
   Identifying and analyzing the current controls.
7. Which of the following is the main benefit of risk-based audit planning?
   the focus on high-risk areas.
8. Which of the following should be the primary focus when considering the level of security of an IT asset?
   the criticality of the IT asset
9. The actions of the IS auditor is most likely to influence which of the following risks?
   detection
10. What is the risk of an inadequate audit methodology known as?
    Detection risk

11. Particular threat of an overall business risk indicated as
    the product of the probability and impact
12. Which of the following is the first step in performing risk assessments of information systems?
    reviewing the threats and vulnerabilities applicable to the data center.
13. What is the first step in evaluating the security controls of a data center?
    evaluating the threats and vulnerabilities applicable to the data center site.
14. What does the classification of information assets help to ensure?
    information asserts are subject to suitable levels of protection.
15. Which of the following should be performed first in a risk-focused audit?
    analyzing inherent risk
16. In a risk-focused audit, which of the following is the most critical step?
    determining high-risk processes.
17. Which of the following options best describes the process of assessing a risk?
    subject-oriented
18. What is the outcome of a risk assessment exercise utilized for?
    implementing relevant controls
19. With whom does the responsibility of managing risk to an acceptable level rest?
    Senior business management
20. Which of the following is a major factor in the evaluation of IT risks?
    finding threats/vulnerabilities associated with current IT assets.
21. An IS auditor has determined a few vulnerabilities in a critical application. What should their next step be?
    identifying threats and their likelihood of occurrence.
22. What does a lack of appropriate control measures indicate?
    vulnerability
23. Which of the following is the first step in a risk management program?
    identifying assets
24. What is the advantage of the bottom-up approach to the development of enterprise policies?
    are created on the basis of risk analysis.
25. The mitigation of risk can be done through which of the following?
    controls

26. The most important factor when implementing controls is ensuring that the control does which of the following?
    helps to mitigate risk
27. The absence of internal control mechanisms is known as what?
    inherent risk
28. Which of the following represents the risk that the controls will not prevent, correct, or detect errors in a timely manner?
    control risk
29. What is the primary consideration when evaluating the acceptable level of risk?
    that all relevant risks must be recognized and documented for analysis.
30. What is the best approach when focusing an audit on a high-risk area?
    perform a risk assessment first and then concentrate control tests on high-risk areas.
31. In a risk-based audit approach, which of the following is the least relevant to audit planning?
    the adoption of a mature technology by the organisation.
32. Which of the following is the most important element for an effective risk-based audit plant?
    risk assessment
33. An IS auditor is conducting a risk assessment as part of risk-based audit planning. What is the primary objective of risk assessment?

    to determine the risks and vulnerabilities impacting different processes.

Audit Project Management

1. Which of the following best describes an audit objective?
   a specific goal that the audit seeks to achieve, such as ensuring compliance with policies or evaluating the effectiveness of controls.
2. Which of the following best describes activities involved in the execution phase of an audit?
   performing audit tests and gathering evidence to support audit findings.
3. The first steps to review a service-oriented application is
   to understand services and their allocation to business processes.
4. An information system audit provides
   reasonable assurance about the coverage of material items.

5. The best sampling method when an IS audit is concerned about fraud is
   Discovery sampling
6. Which of the following is the first step in an audit project?
   Develop an audit plan on the basis of the risk assessment.
7. What is the primary goal during the planning phase of an IS audit?
   to address the audit's objective
8. What is the primary reason for a functional walk-through?
   to understand the business process
9. An IS auditor has a strong suspicion of fraud during a preliminary investigation. What should they do next?
   collect more evidence for further investigation.
10. Which of the following is the first activity to be performed when developing a risk management program?
    Inventory of assets
11. An IS auditor has been assigned to audit a business continuity plan. The same auditor was involved in designing the business continuity plan.
    The IS auditor should provide a disclaimer of conflict of interest to audit management before accepting the audit.
12. Which of the following would be a major concern in the absence of established audit objectives?
    Not being able to determine key business risks.
13. Which of the following is the next step once the audit findings have been identified?
    discuss it with auditee management to gain agreement on the findings.
14. The first step in developing an annual internal IS audit plan is for
    determine the audit universe
15. What will be the immediate step once the business process to be audited is identified?
    to determine the control objectives and activities
16. The prime consideration in determining the objective and scope of an audit is
    the statutory requirements applicable to the organization.
17. Which of the following is the prime reason for performing a risk assessment?
    to provide reasonable assurance about the audit coverage of material items.
18. The first step in the planning phase of an audit is
    conducting a risk assessment

19. What should be the next course of action for an IS auditor once the potential material findings are discovered?
    conduct additional testing
20. Which of the following is the best reason for a senior manager reviewing the work of an author?
    professional standards
21. Which of the following is the best course of action if it is not possible to cover the total audit scope due to resource constraints?
    focus on high-risk areas
22. The most reliable source of information when designing a risk-based audit plan is

    the key business process identified by senior management

Sampling Methodology

1. Which of the following best describes statistical sampling?
   a sampling method that ensures each unit in the population has an equal chance of being selected, based on the laws of probability.
2. Which of the following best describes compliance testing?
   testing that evaluates whether internal controls are functioning as intended and in accordance with established procedures.
3. Which of the following best describes substantive testing?
   testing that focuses on the accuracy and completeness of data, transactions, or financial statements.
4. Statistical sampling is preferred over non-statistical sampling
   when the probability of error must be objectively quantified
5. Which of the following risks can be mitigated by statistical sampling?
   detection risk
6. Which sampling method that will be MOST meaningful for compliance testing?
   attribute sampling
7. Which of the following is correct with respect to confidence correlation?
   the confidence coefficient may be lowered if the author knows that internal controls are stringent.
8. To determine the correct processing of the last 50 new user requisitions, which of the following is best?
   compliance testing

9. The sampling method to be used when there is indication of fraud is
discovery sampling
10. Which sampling method will be best to ascertain the correctness of system access rights as per the approved authorisation matrix?
attribute sampling
11. In the case of a strong internal control, an auditor can adapt a
lower confidence coefficient, which leads to a lower sample size.
12. The best example of a substantive test is
the use of a statistical sample to verify the inventory of a tape library.
13. The difference between compliance testing and substantive testing is that
substantive testing tests the details, compliance testing tests the controls.
14. To determine that only active users have access to a critical system, which of the following is best?
compliance test
15. The substantive test procedure can be reduced, if, after a compliance test, it is concluded that
the risks of control are within acceptable norms.
16. An example of a substantive audit test includes
a review of the accounts receivable for an aged trial balance.
17. Which of the following is the objective of a compliance test?
to ascertain the adequacy, effectiveness, and efficiency of controls.
18. The use of a statistical sample to inventory the tape library is considered as
a substantive test
19. To determine whether the source and object versions are the same, what procedure is performed?
a compliance test of the program library controls
20. Evidence gathering to determine the accuracy of an individual transaction or data is
substantive testing
21. The IS auditor conducting a review to determine the effectiveness of the IT assets procurement process. As part of the review, need to determine whether requisite approvals are in place before procuring IT assets. What is the most effective sampling technique to use?
attribute sampling

22. Reviewing the user access creation process and specifically want to determine approvals for third-party consultants. What is the most appropriate testing methodology?
    Stratified sampling
23. Compliance testing is used to determine

    instances of unauthorised system changes.

Audit Evidence Collection Techniques

1. While gathering audit evidence, the prime focus should be on
   reliability of audit evidence collected
2. The reliability of audit evidence is primarily dependent on
   the source of the evidence
3. The most significant factor that impacts the extent of the data requirements for an audit is
   the objective and scope of the audit
4. While reviewing the implementation of an application, it is observed that the results of penetration are not yet declared and will not be finalised prior to implementation. What is the IS auditor's best option?
5. While reviewing a change management process, it is observer that the number of changes that are available for sampling does not give reasonable assurance. What is the best option for the IS auditor?
   to design an alternative test procedure.
6. Which of the following ascertains the extent of the data requirements for the audit?
   the purpose, scope and objective of the audit
7. Which of the following can be considered most reliable evidence?
   a confirmation letter from a relevant third party
8. The best evidence for the existence of the segregation of duties is
   observation and interview
9. Which of the following can be considered best evidence to determine system configuration settings?
   a configuration report extracted from the system directly by the audit team.
10. Which of the following can be considered the most reliable information?
    IS audit reports

11. The best evidence to determine the effectiveness of control involving the review of system generated exceptional reports is
    a sample exception report along with a follow-up action plan.
12. The best evidence to determine the accuracy of system logic for transaction processing is
    the creation of simulated transactions for processing and comparing results for correctness.
13. An IS auditor should be use professional judgement primarily to ensure appropriate audit evidence will be collected.
14. An IS auditor should ensure that the audit findings are supported by sufficient and appropriate audit evidence.
15. Sufficient audit evidence is obtained
    to provide reasonable basis of drawing a conclusion.
16. The most effective tool for obtaining audit evidence through digital data is CAATs
17. The use of CAAT tool will impact which of the following attributes of evidence? reliability
18. The prime advantage of an audit team directly extracting data from a general ledger system is
    more reliability of data
19. The best evidence to determine the accuracy of system logic for transaction processing is

    re-performance

Data Analytics

1. Which of the following steps will be taken first to carry out data analytics? determining the analytics targets and range
2. The prime benefit of the usage of CAAT is
   it provides reliability for the source of information and thus reassurance on the audit findings.
3. Which of the following is a prime consideration when using CAAT?
   to ensure the integrity of imported data by safeguarding its authenticity, integrity, and confidentiality.
4. The best way to determine the proper functioning of the system calculation is use of CAATs to perform substantive testing

5. The best audit method when an audit trail is required as
   Snapshots
6. An important feature of ITF is
   setting up a separate test environment/test process is not required.
7. ITF is best used for
   the verification of system processing
8. The best continuous auditing technique for the early detection of errors or irregularities is
   audit hooks
9. The best auditing tool to capture transactions as per the predefined criteria is
   CIS
10. An important feature of ITF is
    the results of the test transaction are compared with the predetermined results to validate the system processing.
11. The best technique to identify excess inventory for the previous year is
    Generalised audit software
12. As the Chief IS auditor of HDA Inc., plan to introduce computer-assisted audit techniques (CAATs) to improve audit processes. Evidence evaluated through CAATs will be more

    reliable

Reporting and Communication Techniques

1. Which of the following best describes a follow-up audit?
   a subsequent audit performed to verify that corrective actions have been implemented and are effectively addressing the findings form a previous audit.
2. Which of the following should an IS auditor do when an auditee has taken immediate corrective action of audit findings?
   report the observation and risk in the final report.
3. The best course of action for an audit team if they find prior audit reports without work papers is
   to inform audit management and suggest retesting the controls.
4. An auditor should hold the closure meeting with the objective of
   discussing audit observations
5. An IS auditor is responsible for the communication of audit results to
   senior management and/or the audit committee

6. An auditor should hold the closure meeting with the objective of
   ensuring that there have been no misunderstandings or misinterpretations of facts.
7. Which of the following should be the first action in the case of non-agreement by the department manager over the audit findings?
   revalidate the supporting evidence for the audit evidence.
8. The main reason for meeting with auditees before formally releasing the audit report is to
   gain agreement on the findings.
9. Which of the following should an IS auditor do when they find that a critical DIsaster Recovery Plan (DRP) does not cover all of the systems?
   determine the impact of the non-inclusion of a critical system in the DRP.
10. The main reason for meeting with auditees before formally releasing the audit report is to
    validate the accuracy of the audit findings.
11. Which of the following should an IS auditor do when they observe minor weaknesses in the database that are beyond the scope of the audit?
    report the weakness in the audit report
12. Which of the following should an IS auditor do when they observe major weaknesses in the change management application supporting the finance applications?
    formally report the deficiency in the audit report
13. The prime objective of an audit team discussing the audit findings with the auditee is
    confirming audit findings and proposing a course of corrective action
14. An IS auditor is reviewing a critical application that has not yet been implemented. Certain evidence is not available. The auditor should
    issue the audit report based on the available information, highlighting the potential security weakness and the requirement for follow-up audit testing.
15. An IS auditor has observed inadequate controls of remote access for a critical application. However, auditee management is satisfied with existing controls in form of IDS and monitoring of firewall rules. The auditor should
    document the audit findings in the audit report
16. The audit team should ensure that the audit findings are supported by
    audit evidence

17. Which of the following should an IS auditor do if an auditee does not agree with the audit findings?
    explain the impact of the findings and the risk of not correcting it.
18. The BEST way for an IS auditor to follow up on the closure activities is to conduct a review of the controls after the projected remediation date.
19. To review the adequacy of management's remediation action plan, the most important factor is
    the criticality of the audit findings
20. The BEST way to schedule a follow-up for audit findings is to
    schedule a follow-up audit based on closure due dates.
21. Which of the following is the main objective of conducting follow-up audits?
    to validate the remediation action
22. As part of an integrated audit, reviewing the IT controls of a business process. The primary objective should be

    highlight the business impact due to IT controls failures

Summary

- Auditors can prioritize their efforts and concentrate on areas that are more likely to have significant control deficiencies.
- By identifying and prioritizing high-risk areas within the organisation, auditors can allocate their resources and efforts effectively.
- Understanding threat and vulnerabilities will help auditors to concentrate on high-risk areas.
- Risk-based audit planning is designed to ensure that enough audit resources are spent on the risk-prone areas.
- The audit universe is a list or inventory of all possible audits that could be conducted within an organisation.
- The audit universe encompasses all areas that could be subject to an audit, ensuring comprehensive audit coverage.
- A qualitative risk assessment evaluates risks based on descriptive categories. It helps in prioritizing risks by categorizing them based on factors like likelihood and impact using subjective assessments.

- A quantitative risk assessment uses mathematical models and numerical data to evaluate the probability and impact of risks, providing a more precise and measurable assessment.
- Ideally, top management should approve the audit charter.
- The approved audit charter is the basis on which the chief audit officer carries out audit processes.
- The IS department and the IT steering committee should not be involved in the preparation of the audit charter.
- The overall scope, authority and responsibility of the audit function is outlined in an audit charter.
- The charter should not be frequently modified.
- The audit charter will not cover procedural aspects such as the audit calendar and resource allocation.
- Business continuity arrangements should ideally be incorporated in the BCP document, and it should not form part of the audit charter.
- The main purpose of the audit charter is to define the auditor's roles and responsibilities.
- The audit charter should empower auditors to perform their work.
- Procedural aspects such as audit procedure, resource allocation, and ethical standards should not be a part of the audit charter.
- Audit planning is included in the audit calendar.
- The risk assessment and treatment plan should contain details of identified risks and their mitigating controls.
- The compendium of audit observations contains a summary of critical audit observations for top management.
- An organization chart is used to derive details about the authority and responsibility of relevant functions in the organization.
- It will help to understand whether proper segregation of duties exists.
- Primarily, the actions of the audit team will be influenced and guided by this charter.
- The audit charter should also document the reporting matrix of the audit function.
- Generally, the head of the audit reports to an audit committee.

- The audit charter should be approved by top management/members of the board.
- The overall scope, authority and responsibility of the internal audit department is outlined in the audit charter.
- The authority, scope and responsibilities of the external audit are governed by the engagement letter.
- An internal audit charter is an official document that comprises the internal audit department's objectives, authority, responsibilities and delegation of authority.
- The audit function should be independent of influence and bias.
- Having direct and immediate access to the audit committee can enable auditors to put up major irregularities and concerns without any influence from business functions.
- The audit charter establishes the authority, responsibility, and accountability of the internal audit function, providing it with the necessary framework to operate effectively within the organization.
- By defining the internal audit function's role, the audit charter enhances its credibility and acceptance within the organisation.
- It provides a clear mandate for the audit function.
- Legal liability cannot be enforced in the absence of an agreement between trading partners.
- A dedicated communication channel is considered a good control for Electronic Data Interchange (EDI).
- Encryption is a technical control through which plaintext is converted into encrypted (non-readable) text.
- Encryption processes are implemented to ensure the integrity and confidentiality of transactions.
- Building a segment count total ensures the completeness of inbound transactions in an Electronic Data Interchange (EDI) environment.
- In Key verification, the same field is filled in twice and a machine compares the entries for verification and validation.
- A reasonableness check ensures the logical reasoning of an input transaction.
- The control total is a system-based control that ensures that all relevant data is captured.
- A sequence check ensures the continuity of serial numbers.

- Completeness controls ensure the presence input for all required fields.
- Non-repudiation is a control that ensures that the sender cannot deny a transaction.
- Non-repudiation ensures that a transaction is enforceable.
- A primary area of concern when auditing Electronic Data Interchange-based processes is the lack of controls to ensure transaction integrity.
- Electronic Data Interchange (EDI) transactions are automated and often occur without human intervention, making it crucial to have strong controls in place to verify that transactions are complete, accurate and authorised.
- Preventive controls are incorporated in such a way that prevents a threat event and thus avoids its potential impact.
- Detective controls are implemented to detect threat events once they have occurred.
- Detective controls aims to reduce the impact of an event.
- Corrective controls are designed to minimize the impact of a threat event once it has occurred and help in restoring a business to its routine operations.
- Compensating controls are alternate measures that are employed to ensure that weaknesses in a system are not exploited.
- In many cases, a strong control in one area can compensate for weaknesses in other areas.
- Segregation of duties is an attempt to prevent fraud or irregularities by segregating duties such that no single employee can commit fraud or other irregularities.
- Well-designed documents are an attempt to prevent errors by implementing efficient and effective operational procedures in the organization.
- Employed only qualified personnel is an attempt to prevent errors or other irregularities.
- Check subroutine corrects the error. It modifies the processing system and minimizes the likelihood of future occurrences of the problem.
- A deterrent control is anything intended to warn a potential attacker not to attack.
- Detective controls use that detect and report the prevalence of an error, omission, or malicious act.
- Preventive controls detect problems before they arise. They prevent omissions, errors or malicious acts from occurring.

- Access control aims to prevent access by unauthorized persons.
- Control risk is a term that signifies the possibility that a control will fail to prevent or detect unwanted actions.
- Example of detective controls include audits, hash totals, echo controls and so on.
- Example of corrective controls include business continuity planning, backup procedures and more.
- On the basis of control objectives, an auditor can plan control to evaluate the effectiveness and efficiency of implemented controls.
- An IDS monitors network traffic and alerts administrators of suspicious activities, making it an example of a detective control.
- Implementing strong password policies restricts unauthorized access, is an example of a preventive control.
- Running antivirus software to remove detected malware is an example of a corrective control.
- Placing security cameras in visible locations is intended to deter potential theft, making it an example of a deterrent control.
- The audit objective defines the specific goals the audit seeks to achieve, such as ensuring compliance with regulations, evaluating the effectiveness of internal controls, or verifying the accuracy of financial statements.
- The execution phase of an audit involves performing audit tests, gathering evidence, and evaluating information to support the audit findings.
- This phase is where the bulk of the audit work is performed.
- Service-level architecture relies on the principle of multiple clients.
- The auditor does not provide absolute assurance but only reasonable assurance.
- Absolutes are not attainable due to the inherent limitation of audits, such as professional judgement, sampling and the use of testing.
- Discovery sampling is widely used to detect a fraudulent transaction.
- If one instance of fraud is found, the auditor is confident that fraud exists.
- The first step of the audit project is to develop the audit plan after considering the results of the risk assessment.
- The main reason for a functional walkthrough is to have a basic idea and knowledge about the business process.

- An IS auditor should further evaluate the evidence to decide on the recommendation of a detailed examination.
- The first step in the development of a risk management program is the identification of the assets to be protected.
- It is the responsibility of the IS auditor to communicate any possible conflict of interest to audit management that can impact the IS auditor's independence.
- In the absence of audit objectives, an audit scope cannot be determined and hence a key business risk may not be identified.
- After identifying the audit findings, the IS auditor should gain an agreement on the finding with auditee management.
- The first step in developing an annual internal IS audit plan is to determine the audit universe for the organization.
- Once the audit universe is identified, critical processes and systems are to be identified on the basis of their value to the organization.
- A risk assessment should be done of these critical systems and processes and accordingly, an audit plan should be designed.
- Once the business process to be audited is identified, the next step is to identify the control objectives and activities associated with the business processes.
- The next step is to identify the audit resources.
- The audit universe is to be determined prior to the finalization of the audit scope.
- The prime consideration in determining the objective and scope of an audit is the statutory requirements applicable to the organization.
- The auditor cannot limit the scope relating the statutory requirements.
- A risk assessment is the first step to be performed to allocate audit resources as per the high risks of the organization.
- The best course of action is to perform additional testing to confirm the correctness of the audit findings.
- Only on the basis of sufficient objective evidence should audit findings be reported.
- Findings should be confirmed through additional testing before they are discussed with the business unit or reported to the audit committee.

- The professional standards issued by ISACA, IIA, and the International Federation of Accounts require the review of the work of an auditor by a senior audit manger to ensure that the audit objectives are met and the audit is conducted as per the accepted procedures.
- The best course of action is to reduce the audit scope and to focus on high-risk areas.
- Statistical sampling uses the laws of probability to ensure that each unit in the population has an equal chance of being selected, making the results more reliable and generalisable.
- Compliance testing involves evaluating whether internal controls are functioning as intended and adhere to established procedures, ensuring that policies and regulations are followed.
- Detecting unauthorised changes is a key aspect of this, ensuring that all system modifications are properly authorised and documented.
- Substantive testing involves verifying the accuracy and completeness of data, transactions, or financial statements, ensuring that the financial information is free from material misstatement.
- To objectively quantify the probability of error, there should not be any involvement of subjectivity.
- Detection risk can be minimised by statistical sampling.
- Detection risk is the risk that the auditor may fail to detect material control deficiency.
- For compliance testing, attribute sampling will be most relevant.
- The confidence coefficient, or confident level, is a measure of the accuracy and confidence of the quality of the sample.
- Sampling size and confidence correlation are directly related.
- A high sample size will give a high confidence coefficient.
- When the internal control environment is strong, detail testing is not required and hence a small sample size.
- Compliance testing helps to determine the presence of controls.
- Compliance testing indicates whether controls are being applied consistently.
- Compliance testing helps to evaluate whether new accounts were appropriately authorised.
- Stop-or-go sample is used when only a few errors are expected in a sample.

- Attribute sampling is used for compliance testing and variable sampling is used for substantive testing.
- The attribute sampling method is often used to test whether or not a company's internal controls are being correctly followed.
- To verifying that only active users have access to critical systems requires evaluating the existence of controls and hence a compliance test is used.
- If the outcome of compliance testing indicates the existence of effective internal control, then substantive testing may not be required or may be reduced.
- In substantive testing, evidence is gathered to evaluate the accuracy of the data or other information.
- Attribute sampling is used to determine the presence or absence of specific characteristic (attributes) in a population.
- Stratified sample involves dividing the population into subgroups (strata) and then taking a sample from each subgroup.
- By stratifying the user access creation process by different user categories, it can ensure that the sample includes a sufficient number of third-party consultants for a focused review of their approval process.
- The reliability of audit evidence is paramount as it ensures that the audit findings are based on accurate, credible and dependable information.
- The reliability of audit evidence is primarily dependent on its source.
- Evidence obtained from independent, external and well-documented sources is generally more reliable than evidence from internal or less formal sources.
- The objective and scope of the audit is the best factor to determine the extent of the data requirements.
- A limited scope may not require huge data collection.
- A wider scope may require more data for analysis and sample verification.
- The auditor is not required to conduct a penetration test.
- The purpose, scope, and objective of the audit directly determine the extent of the data requirements.
- It should not be constrained by the availability of information, the experience of the auditor, or the nature of the business.
- A user access review does not provide complete information compared to an interview.
- User access can changed between audits.

- Management assurance and organisation charts can be considered as additional evidence.
- Evidence collected directly from the source by the audit team is considered more reliable compare to the other options.
- An audit report by a qualified author is considered more reliable than a confirmation letter received from a third party.
- A review of the exception report along with a follow-up action represents the best practices evidence.
- It determines that the control process is in place and also follow-up actions are taken for exceptions.
- The most effective evidence is to create simulated transactions for verification.
- Primarily, an IS auditor's professional judgement is required to ensure that sufficient audit evidence is collected.
- An audit need not necessary identify all the deficiencies.
- Auditee management is responsible for taking corrective action.
- Completing an audit within the defined timeline is an important element, but the primary objective of the audit procedure is to collect sufficient evidence.
- The audit team should ensure that their reporting is based on objective evidence.
- Audit evidence helps the IS auditor to draw a conclusion about the subject under audit.
- Audit evidence can be used to trace back the audit finding.
- CAATS are the most effective auditing tools for computerised environments.
- The use of CAAT ensures the reliability of audit evidence as data is directly collected, processed, and analysed by the IS auditor.
- CAAT provides assurance about the reliability of the data.
- In re-performance, a transaction is processed again and results are compared to validate the transaction. This gives the strongest evidence among all the other options.
- When the same results is obtained after performance by an independent person, it provides assurance about the accuracy of the system logic.

- Steps in data analytics
  - Determining the analytics targets and range.
  - The requirement to capture and collect data.
  - Determining the data's adequacy and accuracy.
  - A review of the results/conclusion by a qualified person.
- Substantive testing using CAATs will be the best way to ensure that calculations are performed correctly by the system.
- The snapshots technique captures snaps or pictures of the transaction as it is processed at different stages in the system.
- Details are captured both before the execution and after the execution of the transaction.
- The correctness of the transaction is verified by validating the before-processing and after-processing snaps of the transactions.
- A fictitious entity is created in the live environment. There is no need to create separate test processes as a live environment is used.
- In the ITF technique, a test transaction is entered.
- The processing results of the test transaction are compared with the expected results to determine the accuracy of the processing.
- If the processed results match the expected results, then it determines that processing is happening correctly.
- In the audit hook technique, a code is embedded into the application systems to review the selected transactions.
- The audit team can act at the earliest possible time before an error or an irregularity comes out of hand.
- They have low complexity in the design of criteria and are also very useful for the early identification of fraud or an error.
- CIS is useful for identifying the transactions as per the predefined criteria in a complex environment.
- CIS replicates or simulates the processing of the application system.
- In this technique, the simulator identifies transactions as per the predefined parameters.
- Identified transactions are then audited for correctness.
- CIS decides whether any errors exist between the results it produces and those that the application system produces.

- If any discrepancies are noted, they are written to the exception log file.
- The IS auditor could design suitable tests to identify excess inventory using generalised audit software.
- The test information would not be relevant here as the actual data will need to be audited.
- ITF and EAM cannot identify errors for a previous period.
- CAATs enhance the reliability of evidence by using automated processes to analyse large volume of data accurately and consistently, reducing human error and bias.
- It is advisable to report the finding even if corrective action is taken by the auditee.
- For any action taken on the basis of audit observation, the audit report should identify the finding and describe the corrective action taken.
- The major purpose of the closure meeting is to discuss gaps, conclusions and recommendations.
- This communication helps to address misunderstandings or the misinterpretation of facts.
- The audit team is finally responsible for the communication of audit results to the audit committee of the board and senior management.
- It is the board of directors who should report to legal authorities.
- Closing meeting helps to enhance the understanding between the auditor and the auditee in terms of what was presented, discussed and agreed upon.
- It is advisable to revalidate the supporting evidence first to ensure that the auditor has sufficient objective evidence to support the conclusion drawn.
- The auditor should consider compensating controls, if any, if even after revalidating some disagreement persists,, then it should be included in the report.