ISACA CISA® - Quiz Questions with Answers

Domain 1: Information System Auditing Process

1.

Which of the following is the **BEST** definition of compliance testing?

Gathering evidence in order to test a business's compliance with control procedures

Gathering evidence in order to evaluate the integrity of transactions, data, or other information

Gathering evidence in order to measure the effectiveness and efficiency of controls, primarily by automated processes

Extrapolating characteristics of a large population based on the characteristics of a sample

---

Correct answer: Gathering evidence in order to test a business's compliance with control procedures

The best definition of compliance testing is gathering evidence in order to test a business's compliance with control procedures. For example, an auditor may look at a certain system such as change control and determine whether this is being done properly.

Evaluating the integrity of transactions and data is substantive testing. IS auditing is concerned with the assessment of IS controls. Sampling is used to infer the characteristics of the entire population.

2.

While documenting evidence for an audit, an auditor is observing employees in the performance of their duties. The auditor notices that one employee is doing work that they should not have access to. What category of exception should the auditor note in this scenario?

Actual functions

Actual processes

Security awareness

Reporting relationships

Correct answer: Actual functions

Job functions should be completed by the particular person who is assigned the job. An employee doing another user's job can be a sign of improper logical access rights.

Actual processes refer to not following documented procedures to complete a process. Security awareness refers to employees being trained to practice preventive security measures. Reporting relationships refers to following the hierarchy of authority in an organization.

3.

Which of the following is **NOT** an ISACA IS Audit and Assurance Standards category?

Ethics

General

Performance

Reporting

Correct answer: Ethics

There are three categories of standards and guidelines:

1. *General: The guiding principles under which the IS assurance professional operates, applying to all conduct of the ISACA assignments and encompassing the IS audit and assurance professional's ethics, objectivity, knowledge, competency, and more.*
2. *Performance: Deals with the conduct of the assignment, planning and supervision, scoping, risk, supervision, resource mobilization and assignment management, and audit and assurance evidence.*
3. *Reporting: Covers the types of reports, means of communication, and the info shared or communicated.*

Ethics is not one of three categories of standards and guidelines. It is covered in the Code of Professional Ethics.

4.

Which of the following statements accurately describes the relationship between ISACA standards, guidelines, and the code of ethics?

Audit guidelines are optional, while the standards and code of ethics are mandatory.

Audit guidelines and the code of ethics are optional, while the standards are mandatory.

Audit guidelines, the code of ethics, and standards are all optional.

Audit guidelines and standards are optional, while the code of ethics is mandatory.

Correct answer: Audit guidelines are optional, while the standards and code of ethics are mandatory.

ISACA's ITAF is composed of guidelines, standards, a code of ethics, and tools/techniques. The audit guidelines are optional, while the standards and code of ethics are mandatory.

5.

An ideal annual audit plan would include:

All the processes that are rated "high"

All the processes that are budgeted for within the next year

All the long-term issues

As many new acquisitions as possible

Correct answer: All the processes that are rated "high"

An ideal annual audit plan theoretically includes all the processes that are rated "high." Available resources are often inadequate for the execution of the entire ideal annual audit plan, but an audit plan that includes all "high" processes helps demonstrate to management the gap in resources and gives management an idea of the risks involved.

It is impractical to audit all the long-term issues or as many acquisitions as possible; therefore, they would not be included in an "ideal" annual audit plan.

6.

An auditor is auditing a technology firm that has a lot of proprietary data that should not be leaked. During the audit, the auditor discovers that employees can easily transfer files to USB drives and take them from the office. To address this, the auditor recommends a DLP system. What class of control is the auditor recommending?

- **Preventative**
- Detective
- Deterrent
- Corrective

Correct answer: Preventative

A data loss prevention (DLP) system is a preventative control that actively stops users from exfiltrating data. This can be implemented by analyzing files crossing the network or by monitoring individual systems.

Detective controls only detect exceptions but do not act against them. Deterrent controls try to convince users not to engage in a malicious act. Corrective controls are activated after an unwanted event occurs.

7.

An integrated audit typically includes all the following **EXCEPT**:

Examination in detail of financial transactions

Identification of risks in various areas of an organization

Review of the designs of identified controls

Testing that controls are supported by IT systems

Correct answer: Examination of detailed financial records

The integrated approach seeks to get a complete understanding of an organization by combining operational and financial audits with regard to IS. However, a detailed audit of financials should be completed by financial audit specialists. The integrated audit will focus on the controls in financial departments but not probe into detailed financial transactions.

An integrated audit includes identifying risks, reviewing the design of implemented controls, and testing that controls are supported by IT systems.

8.

An IS auditor is working on a variable sampling because of the sheer number of transactions the organization being audited is performing. The auditor has divided the transactions into groups and drawn samples from each group. This is an ex/ample of which quantitative sampling model?

Stratified mean-per-unit

Unstratified mean-per-unit

Difference estimation

Stop-or-go sampling

Correct answer: Stratified mean-per-unit

Stratified mean per unit is a statistical model where the statistical data in question is broken down into various groups. From these groups, samples are drawn in order to produce a smaller overall sample size relative to the unstratified mean-per-unit.

Unstratified mean-per-unit is a statistical model where a sample mean is calculated and projected as an estimated total. Difference estimation is a statistical model used to estimate the total difference between audited values and book values based on differences obtained from sample observations. Stop-or-go sampling is an attribute sampling method.

9.

Generalized audit software (GAS) usually supports all the following functions **EXCEPT**:

Cybersecurity analysis

Statistical functions

File reorganization

Mathematical functions

Correct answer: Cybersecurity analysis

GAS does not include cybersecurity analysis tools. GAS is software that gives IT auditors independent access to data. It includes features for analyzing information statistically and mathematically.

It enables statistical functions such as sampling, stratification, and frequency analysis. It supports file reorganization by enabling indexing, sorting, merging, and linking with another file. It supports mathematical functions by enabling arithmetic operators.

10.

A risk-based approach can be rather important to a company. What is true about business risk?

It can negatively impact the assets, processes, or objectives of a specific business or organization.

It typically can be ignored and dealt with when needed.

It can be associated with external threats only.

It can be eliminated entirely.

Correct answer: It can negatively impact the assets, processes, or objectives of a specific business or organization.

Risk is the combination of the probability of an event and its consequences. Business risk may negatively impact a company's assets as well as its processes or objectives. The IS auditor is often focused on high-risk issues associated with confidentiality, availability, or integrity. Depending on materiality, sources of risk (internal and external) should be reviewed and mitigated in a timely manner. The higher the risk is, the quicker action should be taken to reduce the risk.

Risks should be adequately managed. It can come from both internal and external sources. Risks cannot be fully eliminated.

11.

An IS auditor has begun planning a review of the security of a financial application used by a Fortune 500 company with campuses all over the world. The application consists of a database with a business logic layer and a web interface overlaying the front end. Users access the application via the local network and from outside the network through a VPN connection.

Which of the following should the auditor do to determine whether the VPN settings require a detailed review?

Perform a risk analysis

Consult the opinion of the IT department

Refer to previous audit documentation and results

Consult ISACA guidelines and best practices

Correct answer: Perform a risk analysis

To determine whether the firewall and VPN configuration should be included in the audit scope, a risk analysis should be performed, and the results should be documented. Details such as software revisions and hardware would be evaluated; if they present a large enough risk, they should be included in the audit scope.

The auditor should not be influenced by individual departments. Previous audit documentation might not be reliable. ISACA provides general guidelines, but a risk analysis has to be completed separately.

12.

Which statement accurately describes the relationship between ISACA's audit standards and ISACA's audit guidelines?

IS auditors are expected to follow the standards, while IS auditors use the guidelines to understand how standards can be implemented.

IS auditors must follow the standards to be legally compliant, while IS auditors use the guidelines to learn how to display proper professional behavior.

IS auditors use the standards to implement rules in the guidelines, while IS auditors use the guidelines for tools and techniques.

IS auditors use the standards for planning, while IS auditors use the guidelines for fieldwork and documentation.

Correct answer: IS auditors are expected to follow the standards, while IS auditors use the guidelines to understand how standards can be implemented.

Two publications from ISACA are the Audit and Assurance Standards and the Audit and Assurance Guidelines. The standards are used to tell auditors the rules they must follow, while the guidelines are used to help auditors understand how to implement the standards.

The Code of Professional Ethics document is used to show proper professional behaviors. ISACA publishes separate tools and techniques for use. Planning, fieldwork, and documentation are phases of an audit.

13.

Which of the following would fall under a detective control classification?

Adding checkpoints in production jobs

Employing only qualified personnel

Using backup procedures

Having disaster recovery planning

Correct answer: Adding checkpoints in production jobs

A detective control works to detect errors and report their occurrence, such as past-due accounts or performing checks on production runs. A CISA candidate should be familiar with the differences between preventive, detective, and corrective controls.

An example of preventive control would be employing only qualified personnel or using encryption software to protect assets. Corrective controls move to minimize the impact of a threat, such as with backup procedures and disaster recovery planning.

14.

An auditor is analyzing the inventory of a computer parts retailer. The retailer is concerned by the greater shrinkage of their inventory compared to what is on the books. What type of methodology can the auditor use to compare a sample of the inventory to the bookkeeping number?

Difference estimation

Stratified mean per unit

Discovery sampling

Stop-or-go sampling

Correct answer: Difference estimation

Difference estimation is used to compare the results of sampling to the results in the books. In this case, the auditor can suspect fraud if the sample points to a number that is different from the number recorded.

Stratified mean per unit divides a population into classes. Discovery sampling is used to detect at least one exception. Stop-or-go sampling can be stopped early before the whole population has been sampled.

15.

All the following are factors that affect an audit, **EXCEPT**:

Hiring a new staff member

Changing market conditions

A merger or acquisition

New regulatory requirements

Correct answer: Hiring a new staff member

Events that result in new business processes or changes to business processes often affect security controls. These changes could require a new audit. However, hiring new staff members should not change business processes.

Changing market conditions could affect supply chains, thereby affecting an audit. Mergers and acquisitions combine two organizations and involve intensive changes to processes. New regulatory requirements, such as GLBA, can affect audits.

16.

An auditor has been asked to perform attribute sampling and should achieve a low precision percentage. What can they do to achieve this?

Use a high sample size

Aim for a low accuracy number

Reduce the tolerable error rate

Set the confidence coefficient to 90%

Correct answer: Use a high sample size

Precision is how closely a sample represents a population. A low precision amount or percentage equates to high accuracy and is achieved by using a larger sample size rather than a smaller sample size.

A low-accuracy number means a high precision percentage. The tolerable error rate is the highest number of errors there can be without a result being materially misstated. A confidence coefficient of 90% is not a high degree of comfort.

17.

Which of the following is **NOT** a basic step for managing and administering audit projects?

Monitor management response

Plan the audit engagement

Execute the plan

Build the audit plan

Correct answer: Monitor management response

The following are basic steps for managing and administering audit projects:

- *Plan the audit engagement*
- *Build the audit plan*
- *Execute the plan*
- *Monitor project activity*

Monitoring management response is not a basic step in managing and administering audit projects.

18.

A company that develops computer hardware is looking to do a voluntary internal audit. What is one advantage of the company performing this self-assessment?

Improves employee awareness of controls

Exempts the company from external audits

Ensures that employees cannot hide fraud

Lessens the workload on current employees

Correct answer: Improves employee awareness of controls

One advantage of a control self-assessment (CSA) is that employees will have more awareness of implemented controls. Other advantages can include detecting risks earlier, improving controls faster, and having a greater sense of ownership of controls.

A CSA does not exempt a company from external audits. A CSA cannot uncover employee fraud if the employees are doing the audit. A CSA may add additional work for current employees.

19.

What is included in ISACA's 2402 (Follow-up Activities) guideline?

Management's proposed actions

Evaluation of sample results

Responding to irregularities and illegal acts

Governance of the admissibility of non-audit services or roles

---

Correct answer: Management's proposed actions

ISACA's follow-up activities include recommendations to ensure that the audit's findings are effectively addressed. The management's proposed actions for this are included in follow-up activities.

Evaluation of sample results is in guideline 2208, Audit Sampling. Responding to irregularities and illegal acts is in guideline 2207, Irregularity and Illegal Acts. Governance of the admissibility of non-audit services or roles is in guideline 2003, Professional Independence.

20.

What is the first step in performing an effective IS audit?

Adequate planning

Gathering shareholder feedback

Presenting a plan to the board of directors and receiving approval

Doing preliminary planning to determine the cost

Correct answer: Adequate planning

The first step in performing an effective IS audit is adequate planning. An effective audit program sets objectives and plans audit procedures to fulfill the audit objectives.

Gathering shareholder feedback occurs during and after the IS audit. The annual audit plan is presented to the board of directors, not individual audits. Although a cost-benefit analysis is occasionally performed for an audit, it is not the first step in this process.

21.

Which type of risk in an audit considers the risk that material errors were not discovered by the IS auditor?

Detection risk

Inherent risk

Sampling risk

Control risk

Correct answer: Detection risk

Detection risk is the risk that an auditor will overlook errors. This is included during a risk assessment at the beginning of an audit to help an auditor use higher sampling rates to improve the chances of detecting errors.

An inherent risk is the risk assuming that no controls have been implemented. A sampling risk is that the sampling technique used will not detect transactions that are not in compliance with the controls. A control risk is that the implemented controls will not prevent the targeted issue.

22.

The CSA lifecycle is an iterative process that starts with identifying and assessing risks. What is the final stage of the CSA lifecycle before returning to the phase of identifying and assessing risks?

Perform control remediation

Conduct a workshop

Develop a questionnaire

Identify and assess controls

Correct answer: Perform control remediation

The final phase of the control self-assessment life cycle is control remediation. In this phase, controls are designed or altered to limit risks.

Conducting workshops is used to create ideas for control remediation. Developing questionnaires is done after identifying and assessing controls. Identifying and assessing controls are done after identifying and assessing risks.

23.

ISACA IS Audit and Assurance Standards contain how many categories?

- **3**
- 4
- 5
- 6

Correct answer: 3

There are three categories of standards:

1. *General: The guiding principles under which the IS assurance professional operates, applying to all conduct of the ISACA assignments and encompassing the IS audit and assurance professional's ethics, objectivity, knowledge, competency, and more.*
2. *Performance: Deals with the conduct of the assignment, planning and supervision, scoping, risk, supervision, resource mobilization and assignment management, and audit and assurance evidence.*
3. *Reporting: Covers the types of reports, means of communication, and the info shared or communicated.*

24.

What occurs during the exit interview of an IS audit?

The auditor discusses findings and recommendations with audited management.

The auditor is asked why they have decided to stop the audit.

The auditor answers questions from the audited organization about how the organization can be more effective.

The auditor presents a list of employees that are no longer needed in the organization.

Corrective answer: The auditor discusses findings and recommendations with audited management.

The exit interview is where an IS auditor discusses their findings and recommendations to the audited management. They should ensure that facts are correct and material, that recommendations are realistic, and that dates for implementing recommendations are agreed-upon.

25.

A business needs to prepare for an official audit to be compliant with the Sarbanes-Oxley Act and also wants specific business processes audited. They want to hire a single auditor to do this audit so they can be prepared for an official audit later. What type of audit describes the work that the auditor will be doing?

Integrated audit

Compliance audit

Operational audit

Financial audit

Correct answer: Integrated audit

An integrated audit combines both a financial audit and an operational audit. A business may want to prepare for official audits by performing an audit before.

A compliance audit does specific tests to meet regulations only. An operational audit evaluates controls in a specific area. A financial audit only covers accounts and financial information.

26.

The Performance and Supervision guidelines of the ISACA IS audit guidelines outline important topics such as documenting work performed and roles and responsibilities. What is **NOT** covered under the ISACA IS auditor guidelines on Performance and Supervision?

Guidance for audit professionals on how to obtain the necessary skills

Performing an audit engagement

Gathering evidence

Formulating findings and conclusions

Correct answer: Guidance for audit professionals on how to obtain necessary skills

Guidance on how to obtain and maintain the necessary competencies of an IS auditor is covered in the Proficiency guidelines. The Performance and Supervision guidelines provide guidance to IS audit and assurance professionals for performing their audit engagement and supervising IS audit members. The guidelines cover:

- *Performing an audit engagement*
- *Roles and responsibilities and required knowledge and skills for performing audit engagements*
- *Key aspects of supervision*
- *Gathering evidence*
- *Documenting work performed*
- *Formulating findings and conclusions*

27.

An auditor identifies missing controls in an organization's network security. How should the auditor handle this situation?

Note the exception but do not remediate it

Decide on the best countermeasure for it

Create a task force to remediate the problem

Aid the organization in implementing countermeasures

Correct answer: Note the exception but do not remediate it

The auditor should not take risks but does not have to implement solutions. The auditor should also be careful about making recommendations, as it can be problematic to influence auditee decisions.

Deciding on the best countermeasures is the responsibility of the audited organization. Creating a task force to remediate the problem is not the responsibility of the auditor. Aiding the organization in implementing countermeasures can compromise the objectivity of the auditor.

28.

Each process in an audit is assessed for qualitative and quantitative risk. A risk is considered high if it results in damage to the reputation of the entity **AND**:

- **takes more than six months to recover**
- takes less than six months but more than three months to recover
- takes less than three months to recover
- requires legal action to recover

Correct answer: takes more than six months to recover

Each process in an audit is assessed for qualitative and quantitative risk. A risk is considered high if it is a process issue that results in damage to the reputation of the entity and takes more than six months to recover. A risk is considered medium if it is a process issue that results in damage to the reputation of the entity and takes less than six months but more than three months to recover. A risk is considered low if it is a process issue that results in damage to the reputation of the entity and takes less than three months to recover.

Risk factors are evaluated based on feedback from the business process owners, and every business will be different. For a retail business, reputation is probably a critical risk factor. If legal action is necessary to recover, the risk could be medium or high; therefore, this is not the correct answer.

29.

An auditor is gathering evidence for an audit of a law firm. As part of the audit process, they are interviewing employees. During the interviews, however, they have trouble getting detailed information from employees. What is a reasonable conclusion that an auditor can make from this?

Employees have been coached to provide the minimum amount of information.

Employees do not have the skills or expertise to perform their job functions.

Employees are too nervous to discuss their jobs in one-on-one interviews.

Employees are changing their behavior due to being observed.

Correct answer: Employees have been coached to provide the minimum amount of information.

If employees only give minimal amounts of information during an interview, the auditor should be aware that they may have been coached by their employer not to divulge information. In this case, an auditor should try more creative means to get the information they need.

It is still likely that employees have the skills and expertise to explain their job functions in detail. Nervousness is not likely to be an issue for disclosing information in an interview. Job observation is not a part of interviewing.

30.

Computer-assisted audit techniques are invaluable to the auditor, but accessing data needs to be done safely. All the following are precautions an auditor needs to take, **EXCEPT**:

A computer operator needs to be on hand to verify the integrity of the system.

The auditor should only have "read-only" access to production data.

Updates should be done in a controlled environment that can isolate the production system and protect it from inadvertent changes.

Where possible, an analysis should be done on data that's been downloaded to a standalone platform.

Correct answer: A computer operator needs to be on hand to verify the integrity of the system.

Computer-assisted audit techniques (CAATs) help auditors in complex environments. A computer operator doesn't need to be on hand to verify the integrity of the system.

Computer-assisted audit techniques always need to be performed on data that's isolated from critical production data. CAATs often provide utilities for creating stand-alone platforms that help protect production data. Another precaution is to use a "read-only" mode if available.

31.

What are the three categories of ISACA IS Audit and Assurance Standards?

General, Performance, Reporting

Overall, Operations, Reporting

General, Tailored, Reporting

General, Ethics, Compliance

Correct answer: General, Performance, Reporting

There are three categories of standards and guidelines:

1. *General: The guiding principles under which the IS assurance professional operates, applying to all conduct of the ISACA assignments and encompassing the IS audit and assurance professional's ethics, objectivity, knowledge, competency, and more.*
2. *Performance: Deals with the conduct of the assignment, planning and supervision, scoping, risk, supervision, resource mobilization and assignment management, and audit and assurance evidence.*
3. *Reporting: Covers the types of reports, means of communication, and the info shared or communicated.*

32.

A healthcare company has recently begun implementing continuous auditing. They have installed audit hooks that create alerts when fraudulent transactions are detected. After running the audit hooks for a week, they discover that the audit hooks have sent numerous alerts for normal transactions.

What type of issue are they having with the audit hooks?

- **False positives**
- False negatives
- True negatives
- True positives

Correct answer: False positives

A false positive is an instance where an event is falsely categorized as an important event. The company should tune its alerts so that there are fewer false positives.

A false negative is when a system misses an important event. A true negative is when a system accurately defines an event as not important. A true positive is when a system correctly identifies an event as important.

33.

To perform an audit of an ATM, the auditor needs to do all the following **EXCEPT**:

Review disaster recovery documents

Review customer identification measures and measures of confidentiality maintenance

Review encryption procedures

Review procedures for retaining files and tracing transactions

---

Correct answer: Review disaster recovery documents

Reviewing disaster recovery documents is not ordinarily part of an ATM audit. An IS auditor needs to review processes for customer identification, review measures to maintain customer confidentiality, review file maintenance and retention systems, review exception reports, review the daily reconciliation process, and review encryption.

34.

The guidelines under the ISACA IS audit category of Performance and Supervision do **NOT** cover which topic?

Assessing materiality

Performing an audit engagement

Key aspects of supervision

Gathering evidence

Correct answer: Assessing materiality

The Performance and Supervision guidelines provide guidance to IS audit and assurance professionals for performing their audit engagement and supervising IS audit members. The guidelines cover:

- *Performing an audit engagement*
- *Roles and responsibilities and required knowledge and skills for performing audit engagements*
- *Key aspects of supervision*
- *Gathering evidence*
- *Documenting work performed*
- *Formulating findings and conclusions*

Assessing materiality is in the Materiality guideline.

35.

Which statement accurately describes a facet of how a control self-assessment (CSA) program is employed?

Standards need to be developed for measuring success in each phase.

Care should be taken to avoid overlap with COBIT methods.

Only auditors should be involved in the design of the control environment.

It will remove the requirement of conducting an internal audit.

Correct answer: Standards need to be developed for measuring success in each phase.

A control self-assessment (CSA) differs from other kinds of assessment programs in that the assessment is made by the staff that is being assessed. When a CSA program is employed, measurements need to be decided. Evaluations are usually conducted through surveys or through workshops.

COBIT can be helpful in providing a framework for a CSA program. The workshops assist in giving employees the tools to design the control environment. However, an internal audit is still responsible for an independent review of these areas.

36.

Which term is a percentage expression that shows the probability that a sample is truly representative of the population?

Confidence coefficient

Difference estimation

Expected error rate

Precision

Correct answer: Confidence coefficient

A confidence coefficient is a percentage expression that shows the probability that a sample is a true representation of the population. A 95% confidence level is generally considered a high level of comfort.

Difference estimation is estimating the difference between audited values and book values. The expected error rate is a percentage of the errors that may exist. Precision is the acceptable range difference between a sample and the actual population.

37.

Which of the following is **NOT** part of the ISACA Code of Professional Ethics?

Assist the stakeholders with any means necessary to ensure they pass any audit

Support the implementation of, and encourage compliance with, appropriate standards and procedures for governance and management

Perform all duties with objectivity, due diligence, and professional care

Serve in the best interest of the stakeholders in a lawful manner

---

Correct answer: Assist the stakeholders with any means necessary to ensure they pass any audit

ISACA has all CISA-certified individuals promise to support the implementation of and encourage compliance with appropriate standards and procedures for governance and management; perform their duties with objectivity, due diligence, and professional care; and serve in the best interest of the stakeholders in a lawful manner.

It does not demand professionals to help a company pass any audit through any means necessary.

38.

An IS auditor is reviewing the specific standards and compliance requirements that need to be met in the systems they will be auditing. The auditor has discovered that the ISACA IS Audit and Assurance Standards are not as stringent as the local regulatory authority. What should the auditor do in this case?

Abide by the more stringent regulations and incorporate them into the audit

Observe ISACA's IS Audit and Assurance Standards, as they are the most appropriate in this case

Create custom standards that average ISACA and regulatory requirements

Work with the local regulatory liaison to determine what requirements are necessary

---

Correct answer: Abide by the more stringent regulations and incorporate them into the audit

There may be situations where the legal/regulatory authority has mandated more stringent requirements than the ISACA IS Audit and Assurance Standards. ISACA states that, in these cases, an IS auditor should ensure compliance with the more stringent legal/regulatory requirements.

39.

When gathering evidence, what can an auditor look at to see security events that have occurred at the audited organization?

Incident log

Risk register

Service level agreements

Operations manuals

Correct answer: Incident log

An incident log shows security incidents that have occurred at the organization. It is an important document to look at while gathering evidence.

A risk register shows identified risks to the organization. Service level agreements (SLAs) are contracts with third parties. Operations manuals are IS system documentation.

40.

An auditor is checking a client's database system to ensure that it has proper controls. The company says that the database administrator is on vacation, so they have a network administrator supply the requested information to the auditor. When trying to get information about data access controls, the network administrator instead sends information on performance.

What issue is the auditor facing with regard to collecting evidence during the audit?

Qualifications of the evidence provider

Independence of the evidence provider

Objectivity

Timing

Correct answer: Qualifications of the evidence provider

When collecting evidence, an auditor needs to work with qualified individuals from the audited organization. Sometimes, an auditee may provide unqualified personnel in an attempt to hide information.

The independence of the evidence provider refers to getting evidence from outside sources. Objectivity refers to evidence that is more objective than subjective. Timing refers to information that may be lost if not collected quickly, such as log files.

41.

What does an integrated audit accomplish?

It combines financial, operational, and IS audit steps.

It combines two different IS audits.

It provides a variation of the administrative audit.

It combines an audit of two different departments.

Correct answer: It combines financial, operational, and IS audit steps.

An integrated audit is a combination of financial, operational, and IS audit steps. It also assesses the overall objectives of the company as they relate to financial information and the safeguarding of assets. It includes substantive audit steps.

42.

Which of the following consists of five principles that were developed by ISACA to provide a comprehensive framework to assist with enterprise governance of information and technology (EGIT)?

COBIT

ITAF

COSO

PMP

Correct answer: COBIT

The COBIT 5 framework is a good-practice framework created by ISACA for information technology management and IT governance. It consists of five principles:

1. *Meeting stakeholder needs*
2. *Covering enterprise end-to-end*
3. *Applying a single integrated framework*
4. *Enabling a holistic approach*
5. *Separating governance from management*

COBIT 5 looks for IT to be governed and managed in a holistic manner for the entire enterprise.

The Information Technology Assurance Framework (ITAF), published by ISACA, establishes standards and provides guidance on the design, conduct, and reporting of IT audit and assurance assignments. COSO and PMP were not developed by ISACA.

43.

An auditor is auditing data storage usage at a marketing firm. Each user does similar work, so the auditor does not expect big differences in the amount of storage space used by each user. In this instance, what sampling methodology would the auditor use to find the average storage per user?

Unstratified mean per unit

Stratified mean per unit

Difference estimation

Attribute sampling

Correct answer: Unstratified mean per unit

An unstratified mean per unit is a statistical model for variable sampling when a population is homogenous. In this scenario, the users are expected to have similar data storage usage, so they do not need to be stratified.

A stratified mean per unit is used when the population should be divided into classes. Difference estimation should be used to compare differences between audited values and book values. Attribute sampling is used to answer "how many" questions.

44.

An auditor is gathering evidence for an audit of an investment firm. They currently want to review all the identified potentials for an incident that could cause harm to the organization. What document should they request from the firm?

Risk register

Incident log

Feasibility study

IS policies

Correct answer: Risk register

A risk is a potential for an incident that can cause harm to an organization. A risk register, or risk ledger, will give insights into the risks that an organization has already identified.

An incident log shows events that have already occurred. A feasibility study is a document that determines the practicality of a venture. IS policies show how management directs their IS departments.

45.

A company does not want to just rely on external auditors for oversight of controls. Instead, they want to transfer some of that responsibility to the control operators within the company. What type of methodology can they use to accomplish this?

CSA

SDLC

BIA

DRP

Correct answer: CSA

A control self-assessment (CSA) is a methodology for an organization to self-regulate its controls, rather than rely on outside help. It does not replace a full audit but can help prepare and give an organization confidence in its own controls.

The software development lifecycle (SDLC) is for developing software securely. A business impact analysis (BIA) helps an organization understand business risks. A disaster recovery plan (DRP) is used to plan for addressing the damage of a disaster.

46.

In a traditional EDI, which function is responsible for transmitting and receiving electronic communications between parties over networks?

Communications handler

EDI translator

Application system

Application interface

Correct answer: Communications handler

A traditional EDI has three functions on each party's side: the communication handler, EDI interface, and application system. The communications handler is responsible for transmitting and receiving electronic communications between parties over networks.

The EDI translator is part of the EDI interface and translates data between formats. The application system includes programs that process the data sent over the network. The application interface is part of the EDI interface that performs data mapping.

47.

During a risk-based audit, audit risk is **NOT** influenced by which factor?

Market risk

Inherent risk

Control risk

Detection risk

Correct answer: Market risk

Audit risk is the risk that information that is collected may have material errors or may not be discovered during the audit. Typically, an IS auditor will understand that risk is influenced by:

- *Inherent risk: The risk level or exposure of the process/entity to be audited without taking into account the controls that have already been implemented; it can occur because of the nature of the business*
- *Control risk: The risk that a material error will not be prevented or detected on a timely basis by the system of internal controls*
- *Detection risk: The risk that the IS auditor won't locate misstatements or material errors*
- *Overall risk: The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred*

Market risk is not considered a risk that influences audits.

48.

An advertising company is seeking a third-party service organization to handle its payroll. As this is a critical function of their company, the leadership wants to be sure that the payroll company has been properly audited. What can they request from the service provider that will increase their confidence in the provider's integrity?

SSAE 18

COBIT

SCARF/EAM

NIST SP 800-53

Correct answer: SSAE 18

A Statement on the Standards for Attestation Engagements No. 18 (SSAE 18) can be performed on third-party service providers, and the results can be transmitted to customers. This can increase the confidence that customers have in their service providers.

COBIT is a framework for IT governance. Systems control audit review files and embedded audit modules (SCARF/EAM) involve the embedding of audit applications directly into applications. NIST SP 800-53 is a catalog of security and privacy controls for federal organizations.

49.

An auditor is auditing a company's password policy and discovers that users are able to create weak passwords and re-use them multiple times. How should the auditor proceed in this situation?

Note the exception that password controls are not strong enough in the report

Immediately report the finding to the audit client management

Examine user passwords for instances of insecure passwords

Perform mitigation of the issue before continuing the audit

Correct answer: Note the exception that password controls are not strong enough in the report

If a situation is discovered that is not an immediate risk, then it should be included in the report.

Immediately reporting findings should only be used with high-risk exceptions. An auditor should not be able to examine user passwords. An auditor should continue with the audit and not fix issues they find.

50.

An auditor discovers that a network resource that contained sensitive documents was left without adequate security controls. However, the resource was not easily noticeable by typical employees on the network. So, the auditor wants to determine if at least one employee accessed the resource, as it could be an indicator of fraud.

What type of sampling technique should they use in this scenario?

Discovery

Judgmental

Variable

Stratified

Correct answer: Discovery

Discovery sampling is used when an auditor wants to find at least one exception in a population. If one instance of accessing a sensitive document is found, then more intensive investigations can follow.

Judgmental sampling involves making decisions about which users to audit. Variable sampling is used to determine "how much" of an occurrence is present in a population. A stratified sampling divides the population into classes based on attributes.

51.

All the following are examples of variable sampling models **EXCEPT**:

Sampling used to answer the question "How many?"

Sampling in which the sample population is segmented and samples are selected based on segments

A model where the sample mean is projected as an estimated total

A model estimating the difference between book value and audited value based on differences found in sample observations

---

Correct answer: Sampling used to answer the question "How many?"

Sampling used to answer the question "How many" is attribute sampling, not variable sampling. For example, it can be used to sample data inputs to see if they have been entered correctly.

Segmenting the population is stratified mean-per-unit sampling. Projecting a sample mean as an estimated total is unstratified mean-per-unit sampling. Estimating the difference between book value and audited value is a difference estimation. These three examples are variable sampling models.

52.

Which of the following would fall under the preventive control classification?

Employing only qualified personnel

Checkpoints in production jobs

Secure code reviews

Disaster recovery planning

Correct answer: Employing only qualified personnel

Each CISA candidate should be familiar with the differences between preventive, detective, and corrective controls. For example, a preventive control would employ only qualified personnel.

A detective control works more to detect the error and report the occurrence, such as past-due accounts, checkpoints in production jobs, and secure code reviews. Corrective controls minimize the impact of a threat, such as with disaster recovery planning.

53.

After the audit subject is determined, what is the next phase of the audit process before setting the audit scope?

Defining the audit objective

Performing pre-audit planning

Determining audit procedures and steps for data gathering

Describing how the reporting will be done

Correct answer: Defining the audit objective

After identifying the area to be audited, the next step is to define the audit objective. In this step, the purpose of the audit is given, such as being required by regulations.

Pre-audit planning occurs after setting the audit scope. Determining audit procedures and steps for data gathering occurs after pre-audit planning. Describing how the report will be made can be done in the later stages of the audit.

54.

An auditor wants to use sampling to find the average value for network usage of users in an organization. What type of value are they trying to find?

Sample mean

Sample standard deviation

Tolerable error rate

Sampling risk

Correct answer: Sample mean

A sample mean is the sum of all sample values divided by the size of the sample. This gives the average value for all users.

The sample standard deviation is the variance of the sample values from the sample mean. A tolerable error rate is the highest number of errors there can be without being materially misstated. The sampling risk is equal to one minus the confidence coefficient.

55.

Which of the following is **NOT** a way to treat risk?

Ignore it

Accept it

Avoid it

Transfer it

Correct answer: Ignore it

The proper ways to deal with risk in a risk-based audit are as follows:

- *Risk mitigation: Try to deal with the risk before it can even happen*
- *Risk acceptance: Weigh the outcomes, consequences, and costs of the risk against other efforts to avoid, mitigate, or transfer it*
- *Risk avoidance: Avoid operations that expose the risk in the first place*
- *Risk transfer: Transfer the risk by moving it to services such as insurance or suppliers*

56.

After an audit, the auditor wants to implement quality assurance for the organization. Which of the following is an approach to improving processes and controls?

CSA

ITF

CIS

ERP

Correct answer: CSA

Control self-assessment (CSA) is a form of assessment used by staff and management to assure that controls are adequate. It is a way for an organization to take the initiative in managing its risk rather than engaging outside experts.

Integrated testing facility (ITF) and continuous and intermittent simulation (CIS) are forms of continuous auditing. Enterprise resource planning (ERP) is software that integrates business processes.

57.

Which of the following is **NOT** covered under the Irregularities and Illegal Acts standard?

Follow up to determine whether management has taken steps to address the issues

Planning for and considering the potential for irregular and illegal activity

Exercising professional skepticism

Reporting irregular and illegal acts to the appropriate parties in a timely manner

---

Correct answer: Follow up to determine whether management has taken steps to address the issues

The Irregularity and Illegal Acts standard addresses the consideration and handling of irregular and illegal acts during an audit. As each company is different, it is important to recognize that irregular acts are likely, and there may also be illegal activity. This standard states that an audit professional should expect and consider irregularities and illegal acts, exercise professional skepticism to ensure no bias or overlook, and document and report any material irregularities or illegal acts to the appropriate party in a timely manner.

Following up after an audit is part of the Follow-Up Activities standard.

58.

POS systems allow data to be captured when a sales transaction takes place. What does an IS auditor need to determine?

Whether credit card information is stored on the local POS system

If the system is EFTPOS

How POS information is translated

How long POS transactions are retained on the system

Correct answer: Whether credit card information is stored on the local POS system

If credit card-holder information is stored on a local POS device, it needs to be encrypted with strong encryption methods, and other security measures may need to be installed. Sensitive customer data must always be protected.

Whether the system is EFTPOS, how information is translated, and how long transactions are retained do not need to be audited.

59.

What is the difference between an internal and an external audit?

An internal audit is performed by personnel of the auditee organization, while an external audit is performed by auditors not employed by the auditee.

An internal audit is an audit of an internal network, while an external audit is an audit of the outside network.

An internal audit is a compliance audit, while an external audit is an operational audit.

An internal audit examines the auditee's financial processes, while an external audit examines the auditee's administrative effectiveness.

Correct answer: An internal audit is performed by personnel of the auditee organization, while an external audit is performed by auditors not employed by the auditee.

Internal and external refer to the relationship between the auditor and the audited organization. Typically, an external audit can be expected to be more objective.

The terms "internal" and "external" in regard to auditing do not refer to the network, compliance, operations, financials, or administration.

60.

Which useful technologies for e-commerce can store and enclose any kind of information so that it can be passed between different computing systems?

XML

HTML

CSS

PCI DSS

Correct answer: XML

One of the most useful technologies in e-commerce is provided by XML, which can store and enclose any kind of information so that it can be passed between different computing systems.

XML, or extensible markup language, can store and enclose information and is an important method of exchanging data on the web. Web services are an important offshoot of XML as they represent a way of using XML format information to remotely invoke processing. Web services are now perhaps the most important middleware for connecting distributed web systems and are dependent on XML.

HTML is for formatting content for web browsers. CSS is used to style web pages. PCI DSS is for compliance.

61.

An IS auditor has to review the security of financial applications used by a Fortune 500 company. As part of the audit, they will need to send test transactions to the system to see whether the expected results are returned. Additionally, they will identify if there are any known vulnerabilities in the software used by applications.

What can the auditor use to help automate these tasks?

- **CAATs**
- SCADA
- CSAs
- SLOC

Correct answer: CAATs

Computer-assisted audit techniques (CAATs) help an auditor in complex computing environments. They can perform functions such as analyzing data extracted from databases, running test transactions, scanning software, and utilizing testing scripts.

SCADA is used to monitor and control industrial infrastructure. Control self-assessment (CSAs) is a methodology for reviewing business objectives, risks to achieving the objectives, and controls put in place for them. Source lines of code (SLOC) are used to size software projects.

62.

An auditor wants to determine how much data on average is being sent across a network per user. Which type of sampling method should they use?

Variable

Attribute

Discovery

Stratified

Correct answer: Variable

Variable sampling is used to answer "how much" questions. In this scenario, the variable is how much data each user in the population sends across the network.

Attribute sampling is used to answer "how many" questions. Discovery sampling is used to find at least one exception in a population. Stratified sampling divides a population into different classes.

63.

What is non-statistical sampling?

Sampling based on the auditor's judgment as to what kind of samples to evaluate, the sample size, and the sampling method

Sampling using location to select the sample items to evaluate

Sampling basing sample item selection on polling data and census data, with sample size based on the size of the geographical area

Sampling where the method is based on the auditor's estimation of how precisely the sample needs to represent the population

---

Correct answer: Sampling based on the auditor's judgment as to what kind of samples to evaluate, the sample size, and the sampling method

In non-statistical sampling, the auditor bases their decision on which kinds of transactions are most relevant and most likely to create risk. Statistical sampling is objective and non-statistical sampling is subjective. Statistical sampling needs to be mathematically quantifiable.

Items such as location, size, and representation are not part of the definition of a non-statistical sample.

64.

A start-up company has never had an audit before. They want to make sure that they are prepared for a compliance audit that they have to perform before the end of the year. What can they do to get a better idea of their compliance before they are officially audited?

Undergo a pre-audit

Develop a disaster recovery program

Perform a reasonableness check

Create a reciprocal agreement

Correct answer: Undergo a pre-audit

A pre-audit can be performed to help prepare for an official audit. The results of the pre-audit can be used to implement controls that will give a better result in the real audit.

Developing a disaster recovery program should be done regardless of preparing for an audit. Performing a reasonableness check is for comparing data to expected values. Creating a reciprocal agreement is agreeing with a third party to help each other in a disaster.

65.

An IS auditor needs to review the access controls to a database system. They want to determine whether users are accessing data that they are not authorized to use. Rather than sample all users equally, the auditor wants to focus on the users with the highest levels of access. These users would pose the greatest threat if they have been accessing data beyond their authorization level.

In this case, what type of sampling will the auditor be using?

Non-statistical sampling

Statistical sampling

Stop-or-go sampling

Discovery sampling

Correct answer: Non-statistical sampling

In this example, the best choice would be non-statistical sampling, which uses judgments to determine the method of sampling. This lets the auditor make subjective decisions to audit the riskiest behaviors.

Statistical sampling is objective and uses mathematical laws of probability. Stop-or-go sampling is designed to stop sampling at the earliest possible time. Discovery sampling is used to determine if the entire sample is tainted based on one discovered example.

66.

An organization has a control objective of protecting information from unauthorized personnel. During an audit, the auditor discovers that the organization does not have motion sensors monitoring server rooms where sensitive information is stored. How should the auditor handle this situation?

Evaluate for compensating controls

Report it as a control weakness

Recommend a brand of motion detectors to the client

Immediately disclose the finding to the audit committee

Correct answer: Evaluate for compensating controls

A control objective is not always addressed by a single control. Likewise, many controls can work together as a compensating control. If the client does not have motion detectors, they may have other controls such as video surveillance or door locks.

Reporting as a control weakness should happen if there are no compensating controls. An auditor should not recommend certain brands to a client. This situation does not need immediate disclosure to the audit committee.

67.

Which of the following is an IS-specific control?

Database administration controls

Internal accounting controls

Operational controls

Administrative controls

Correct answer: Database administration controls

General controls apply to all areas of an organization. General controls can be broken into IS-specific controls that ensure the general control is being met. Database controls can be used to meet the needs of general controls, such as safeguarding financial records.

General controls include internal accounting controls, operational controls, administrative controls, and overall policies.

68.

Which type of audit is used to gather evidence after fraud or a crime has occurred?

Forensic

Administrative

Functional

Financial

Correct answer: Forensic

A forensic audit is used to follow up after fraud or a crime has occurred. It requires strict adherence to procedures so that evidence can be used in court.

An administrative audit examines efficiency within an organization. A functional audit checks that software works as intended before being released. A financial audit examines an organization's accounting.

69.

What is true about continuous auditing?

Involves a minimal time-lapse between the collection of evidence and the audit reporting

Is more prone to errors than traditional auditing

Is less efficient at monitoring financial issues

Is attractive to a lot of companies because it involves less work than traditional auditing

---

Correct answer: Involves a minimal time-lapse between the collection of evidence and the audit reporting

Continuous auditing involves a minimal time-lapse between the collection of evidence and the audit report.

It is not inherently more error-prone than traditional auditing. It is more efficient at monitoring financial issues. However, it involves a large amount of work and additional expenses are incurred for additional employees, training, and software applications/subscriptions.

70.

E-commerce presents risks not present in other forms of commerce. The most important risks include all the following **EXCEPT**:

Lack of middleware

Availability

Non-repudiation

Integrity

Correct answer: Lack of middleware

There is no lack of middleware for connecting heterogeneous technologies.

The most important dangers of e-commerce are confidentiality, with customer concerns about providing personal information to unknown vendors and the transmission of data over uncontrolled paths; integrity, or the vulnerability of data to alteration; availability, or the serious consequences of a system failure; authentication and non-repudiation, or protection against one party in the transaction denying that a transaction took place; and the power shift to customers, or the difficulty for e-businesses of enhancing services and competing successfully.

71.

Which continuous auditing technique inserts test transactions into a production system to monitor how the system is working?

ITF

SCARF/EAM

CIS

Audit hook

Correct answer: ITF

Integrated test facility (ITF) is a continuous auditing technique that involves inserting "dummy" test records that can be processed alongside normal transactions. This can help an auditor test the accuracy and completeness of the system.

Systems control audit review file and embedded audit modules (SCARF/EAM) involves embedding audit software into an application. Continuous and intermittent simulation (CIS) involves simulating transactions on another system before running them in production. Audit hooks are inserted into systems to generate alerts when certain events occur.

72.

An auditor has presented their report with findings, conclusions, and recommendations. The auditor would like to check that management has implemented the recommended actions at a later time. What type of program should they implement to confirm that corrective actions have been taken?

Follow-up activities

Continuous auditing techniques

Interviews

Data analytics

Correct answer: Follow-up activities

After the audit report has been submitted, follow-up activities should be scheduled to ensure that recommendations were implemented. This may involve auditing at a later time to verify.

Continuous auditing techniques are used to constantly check systems. Interviews are used to gather evidence. Data analytics is used to detect anomalies or points of interest.

73.

The guidelines for the Audit Charter do **NOT** provide which of the following definitions?

Policies for reporting fraud

Purpose of the audit

Responsibility of the IS auditors

Authority of the IS audit

Correct answer: Policies for reporting fraud

The purpose of the Audit Charter guidelines is to assist an IS audit and assurance professional in designing and crafting an audit charter. The audit charter will define the purpose, responsibility, authority, and accountability of the IS audit and assurance function.

Fraud is covered in the ISACA standard for Irregularity and Illegal Acts.

74.

An IS auditor is reviewing an information system for a risk-based audit. They are logging audit risks to perform classification. The enterprise manually reviews the server logs and is likely to contain errors due to the volume of information being logged. This would fall under which of the following?

Control risk

Inherent risk

Detection risk

Sampling risk

Correct answer: Control risk

Control risk relates to the risk that a material error exists that would not be prevented or detected within an appropriate time period by the system of internal controls. In this example, the control risk associated with reviewing the server logs would be high due to the sheer amount of information being logged by the system.

Detection risk is the risk that material errors or misstatements will not be detected by the auditor. Inherent risk is the risk that something will occur without considering implemented controls. Sampling risk is the risk that the sampling method will not detect issues.

75.

An auditor is analyzing an organization's records related to user login and logout activity. While gathering and examining samples, they notice some logins from the same users coming from different IP addresses at different times during work hours. They want to determine how many users are doing this. What type of sampling approach should they use?

Attribute

Judgmental

Stop-or-go

Discovery

Correct answer: Attribute sampling

Attribute sampling is used to answer "how many" questions related to a given population. In this situation, the auditor wants to find out how many users are logging in from multiple IP addresses.

Judgmental sampling is subjective based on the auditor's risk perceptions. Stop-or-go sampling is used to stop the sampling when there is a low risk of occurrence. Discovery sampling is used to find at least one exception.

76.

The typical audit phases include all the following **EXCEPT**:

Brainstorming phase

Planning phase

Fieldwork and documentation phase

Reporting phase

Correct answer: Brainstorming phase

The typical audit phases include:

- *Planning phase*
- *Fieldwork and documentation phase*
- *Reporting phase*

The brainstorming phase, while a step in the planning phase, is not a typical audit phase.

77.

A cloud service provider has a complex logical security system with its internal employees. They want an auditor that will look into this issue in detail. What type of audit do they need?

Operational audit

Compliance audit

Financial audit

Integrated audit

Correct answer: Operational audit

An operational audit evaluates the controls in a specific process of the organization. It can look at the management of the process or the process itself.

A compliance audit checks for regulatory standards. A financial audit relates to an organization's accounting systems. An integrated audit combines a financial and operational audit.

78.

Which standard in the ISACA IS Audit and Assurance Standards document covers the placement of an auditor in an organization so that they can work objectively?

Organizational Independence

Professional Independence

Reasonable Expectations

Due Professional Care

Correct answer: Organizational Independence

The Organization Independence standard concerns the placement of the auditor within the organization. The auditor should be placed to ensure they can work independently.

The Professional Independence standard concerns the behavior of the auditor. The Reasonable Expectations standard concerns the scope of the audit. The Due Professional Care standard concerns following applicable standards.

79.

Audit documentation should include all the following, **EXCEPT**:

Steps taken as a result of audit recommendations

Audit findings and recommendations

Audit steps performed

Planning of the audit

Correct answer: Steps taken as a result of audit recommendations

Audit documentation wouldn't ordinarily include steps taken as a result of the audit.

The audit documentation includes the audit planning, steps performed, and conclusions and recommendations.

80.

Laws and regulations control audit plans in what way?

The audit plan must adhere to, and test for, all applicable regulations to ensure a company is compliant.

They affect the auditor's behavior to protect the auditor from criminal liability.

They force an auditor to find ways to work around more compliance problems.

They can force an auditor to use less-than-professional methods.

Correct answer: The audit plan must adhere to, and test for, all applicable regulations to ensure a company is compliant.

Well-designed audit plans are created to ensure a company is successfully compliant with all laws and regulations to avoid fines and punitive actions. This is one of the driving factors as it can gravely affect a company's operating capability. In some cases, a business can be closed if it was not properly following regulations.

Laws and regulations do not protect the auditor from criminal liability, force the auditor to work around complex problems, or force an auditor to perform less-than-professional methods.

81.

What is a risk-based audit approach?

Used to assess risk and to assist an IS auditor in making the decision to perform either compliance or substantive testing

A way to address and remove all risk from an engagement

Typically tailored to resolve all risky issues

A definition of how much allowable risk can occur

Correct answer: Used to assess risk and to assist an IS auditor in making the decision to perform either compliance or substantive testing

A risk-based audit approach is used to assess risk and to assist an IS auditor in making the decision to perform either compliance or substantive testing. The risk-based audit approach efficiently assists the auditor in determining the nature and extent of testing. It does not remove or resolve all risks and is not a definition of risk tolerance.

82.

What does the audit scope identify?

The specific processes or systems that will be audited

The type of audit that will be performed

The purpose of the audit

The broad area to be audited

Correct answer: The specific processes or systems that will be audited

The audit scope refers to the specific systems, functions, or units of an organization that will be reviewed. Setting the scope will help determine the technical skills and resources that will be needed for the audit.

The type of audit refers to a financial, IS, or other category of audit. The purpose of the audit is called the audit objective. The broad area to be audited is called the audit subject.

83.

An audit report typically contains all the following **EXCEPT**:

A synopsis of prior audit reports summarizing shortcomings and implementation failures

The auditor's reservations about the audit

Recommendations

Minor findings, which may also be presented to management in the form of a memorandum

---

Correct answer: A synopsis of prior audit reports summarizing shortcomings and implementation failures

A report doesn't usually include anything about prior audits, although a follow-up program is advisable. An audit report should be balanced, including both negative and positive findings. Ultimately, what to exclude or include in the report is based on the auditor's best judgment.

An audit report typically includes an introduction, audit findings, an overall conclusion and opinion, reservations or qualifications, and detailed findings and recommendations (including both material and minor findings).

84.

An auditor starts auditing an electronics retailer. The retailer has numerous stores spread over a single state. The audit client gives the auditor a list of the specific stores where they want transactions audited during the field section of the audit. How should the auditor respond?

Inform the audit client that a sampling method will be used to audit the stores

Accept the audit client's request to audit the specific stores

Notify law enforcement officials of the request

Only audit the stores that were not included in the client's list

---

Correct answer: Inform the audit client that a sampling method will be used to audit the stores

The audit client should not select the sample population to be audited. The auditor should choose an appropriate sampling methodology independently.

The audit client should not choose the specific stores to follow. Law enforcement does not need to be notified. The stores selected for an audit should be based on a sampling methodology.

85.

Due to the growing dependency on info systems and technology, countries have needed to enact legal regulations concerning IS audits. Which of the following is **NOT** an area pertaining to the regulations?

Dictating the criteria for hiring

Establishment of regulatory requirements

Responsibilities assigned to corresponding entities

Financial, operational, and IT audit functions

Correct answer: Dictating the criteria for hiring

As regulation is tightly defined across several industries (e.g., banking, financial, insurance, and health care) it is extremely important for IS audits to take this into consideration. These laws and regulations, such as HIPAA and the Sarbanes-Oxley Act, were enacted by governments in order to better regulate how industries operate and protect consumers and patients.

Dictating the criteria for hiring is not included in the content of legal regulations.

86.

An IS auditor should ensure that proper audit planning has been performed. Which of the following is an incorrect statement about audit planning?

Risk analysis should be performed after the audit plan to ensure completeness.

Reviewing prior work papers can provide valuable insight.

Assigning personnel resources to the audit should be performed during planning.

The audit approach or strategy should be developed during the initial stages.

Correct answer: Risk analysis should be performed after the audit plan to ensure completeness.

Risk analysis should be performed before the planning as it will aid in the process and limit the scope of where the audit should be conducted.

Reviewing prior work is invaluable due to the context and the complexity involved with some business processes, which in large organizations require an in-depth understanding of the individual elements. Personnel used in the audit should be designated and assigned during audit planning. Finally, the approach or strategy is important to develop from the outset to ensure that it is maintained throughout the process.

87.

An auditor is trying to determine how well personnel at an organization have access to information about the IT processes they perform. What can they review to learn about this?

IS policies and procedures

Third-party contracts

Incident logs

Organization chart

Correct answer: IS policies and procedures

To learn about the information available to personnel, the auditor should review IS policies and procedures. This can also show the tone and direction set by management for personnel.

Third-party contracts can give information about business processes. Incident logs give information about incidents that have occurred. An organization chart shows the chain of command and job roles in an organization.

88.

The preventive control classification includes all the following functions **EXCEPT**:

Minimizing the impact of threats

Protecting against malicious acts

Monitoring operations and inputs

Attempting to anticipate problems and make adjustments before they occur

---

Correct answer: Minimizing the impact of threats

The preventive control classification includes protecting against malicious acts, monitoring operations and inputs, attempting to anticipate problems, and making adjustments before they occur.

The preventive control classification does not include minimizing the impact of threats. Minimizing threat impacts is a corrective measure, not a preventive measure.

89.

An auditor is engaged in auditing an insurance company. During the course of their audit, they have amassed a trove of work papers. To keep those documents safe, they have implemented access control and encryption. What other control should they enact to help protect the work papers?

Backup

Version control

Sampling

Indexing

Correct answer: Backup

Workpapers need to be backed up regularly, in addition to having access controls, encryption, and protection from tampering. This will ensure integrity when it is time to produce a report.

Version control is used in software development. Sampling is used for analysis. Indexing is used to speed up searches.

90.

What are the three general requirements for EDI to function?

Communications software, translation software, and access to standards

Web services, a wired network, and a database

Transmission, translation, and storage

Inbound transactions, outbound transactions, and log files

Correct answer: Communications software, translation software, and access to standards

An electronic data interchange (EDI) requires communications software, translation software, and access to standards. An EDI system needs communication software, translation software, and access to standards. Communications software is used to move data from one point to another. It also flags the start and end of an EDI transmission. Translation software is used for building a map that shows how the data fields correspond to elements in an EDI standard.

A map converts data between the application and the EDI. There are specific EDI standards for commonly transmitted forms, such as invoices, purchase orders, and advanced shipping notices. EDI needs to access these standards to know what kind of map to build.

91.

What is the purpose of operational CRM?

To maximize a customer service experience while also capturing useful information about the customer interaction

To analyze information about customers and their interactions with the business and organize this information into data that allow greater value to be obtained from the customer base

To manage the flow of goods, services, and information between two or more organizations

To capture the knowledge and experiences of individuals to perform specific functions

---

Correct answer: To maximize a customer service experience while also capturing useful information about the customer interaction

Operational customer relationship management (CRM) involves direct interaction with a customer. It includes things like call centers and the website itself. Information gathered is used for things like customer classification, sales campaigns, and marketing.

Analytical CRM analyzes information about customers and their interactions with the business and organizes this information into data that allow greater value to be obtained from the customer base. Supply chain management oversees the flow of goods, services, and information between two or more organizations. AI captures the knowledge and experiences of individuals to perform specific functions.

92.

Which of the following is the purpose of the ISACA IS Audit and Assurance Guidelines?

To provide guidance and additional information on how to comply with the ISAC IS Audit and Assurance Standards

To provide a rigid framework to base audit work on

To implement stringent requirements on audits

To provide templates and plans for auditing

Correct answer: To provide guidance and additional information on how to comply with the ISACA IS Audit and Assurance Standards

The ISACA IS Audit and Assurance guidelines work hand in hand with the ISACA IS Audit Standards, providing guidance and much more information on how to tailor an audit toward compliance with the Audit Standards. Adhering to the guidelines makes it much easier to stay within the standards set forth by ISACA.

The ISACA Audit and Assurance Guidelines are used for consideration but are not rigid, stringent, or templates for auditing.

93.

There are three primary goals for an IS auditor when evaluating EDI: inbound transactions are translated accurately, they are passed to an application, **AND**:

They are processed only once

They contain an electronic signature

They are encrypted

Unusual transactions are reported

Correct answer: They are processed only once

The IS auditor must ensure that transactions are translated accurately, passed to an application, and processed only once.

The IS auditor must also review internet encryption, edit checks, additional computerized checking, the logging of each inbound transaction, the use of controlled totals, the use of segment count totals, the batch control totals, and the validity of the sender as a trading partner.

94.

To help analyze data across a variety of information systems, what have IS auditors started using?

CAATs

PERT

SPICE

SaaS

Correct answer: CAATs

Computer-assisted audit techniques (CAATs) are used by an auditor because of the diversity of hardware and software used by organizations. They can perform functions such as database extraction, test transactions, debugging, and scanning.

Project Evaluation and Review Technique (PERT) is a visualization of a project plan. Software Process Improvement and Capability dEtermination (SPICE) is a maturity model. Software as a service (SaaS) is a cloud-based service framework.

95.

Which of the following is **NOT** a step that an auditor may perform to determine an organization's level of compliance?

Examine files with trade secrets or proprietary information

Identify the appropriate government and industry regulatory requirements

Document applicable laws and regulations

Review internal documentation for evaluation of adherence to applicable laws

---

Correct answer: Examine files with trade secrets or proprietary information

An IS auditor attempts to collect all requirements and necessary regulations for a company during audit planning to include the necessary processes in the actual audit. This involves researching and identifying the appropriate laws and regulations applying to a company, documenting those identified, and then applying those requirements to the audit to ensure the company is complying with all the necessary laws and regulations.

An IS auditor should adhere to ethical and professional standards when auditing, which can include not looking at private or sensitive data that are not related to compliance.

96.

What is the final phase of a typical audit process?

Reporting

Planning

Fieldwork

Documentation

Correct answer: Reporting

An audit can be divided into key steps across three distinct phases. The last phase is the reporting phase, which includes gathering report requirements, drafting the reports, issuing the report, and following up.

Planning the report is the first phase. Fieldwork and documentation are put together in the second phase.

97.

Audit conclusions should be supported by reliable and relevant evidence. This would include which of the following?

Observing employees performing their duties

System settings that a system administrator copies to a spreadsheet

A reported conversation that took place between two bank executives

A written report by a computer operator of an incident in the computer room

---

Correct answer: Observing employees performing their duties

Audit conclusions should be supported by reliable and relevant evidence. The key concept of "techniques for obtaining evidence" includes "interviewing and observing personnel in the performance of their duties."

Firsthand information and information gathered as a result of direct observation are always preferable to secondhand information. A reported conversation, a written report of an incident, and system settings copied to a spreadsheet by an administrator are all considered secondhand information. Secondhand information is not considered reliable or relevant evidence.

98.

The ISACA IS audit standard Engagement Planning does **NOT** cover which topic?

Ensuring auditors possess skills in the subject being audited

Sufficiency of scope to meet needs

Compliance with applicable laws

Use of a risk-based approach when needed

Correct answer: Ensuring auditors possess skills in the subject being audited

Engagement planning involves audit planning work to ensure the scope and breadth of an audit are sufficient to meet the organization's needs, that it is in compliance with applicable laws, and that it is risk-based.

Ensuring auditors possess skills in the subject matter being audited is in the Proficiency guidelines.

99.

Which of the following statements is true of population standard deviation?

It can be applied to variable sampling but not attribute sampling formulas.

It can be applied to attribute sampling but not variable sampling.

It can be applied to both attribute sampling and variable sampling.

It cannot be used with attribute sampling or variable sampling.

Correct answer: It can be applied to variable sampling but not attribute sampling formulas.

Population standard deviation is a measurement of the variance of values from a mean. A high standard deviation is associated with a large sample size.

It is not used with attribute sampling, which determines whether a specific quality is present on a binary (yes/no) basis.