PREFACE

ISACA is pleased to offer the 1,000 review questions in the *CISA® Review Questions, Answers & Explanations Manual 12th Edition*. The purpose of this manual is to provide the Certified Information Systems Auditor (CISA) candidate with sample questions and testing topics to help prepare and study for the CISA exam.

This manual includes 1,000 multiple-choice study questions, answers and explanations, which are organized according to the newly revised CISA job practice domains. These questions, answers and explanations are intended to introduce CISA candidates to the types of questions that may appear on the CISA exam. They are not actual questions from the exam. This manual also contains a 150-question sample exam, which has the same proportion of questions related to each CISA job practice domain as the actual exam.

The candidate also may want to obtain a copy of the *CISA® Review Manual 27th Edition*, which provides the foundational knowledge of a CISA. The CISA® Review Questions, Answers & Explanations Database–12-Month Subscription contains the same questions found in this manual in a web-based application. Finally, the candidate may also want to use the CISA® Online Review course or CISA virtual or live instructor-led training for exam preparation.

A job practice study is conducted periodically to ensure that the CISA certification is current and relevant. Further details regarding the new job practice is in the "New–CISA Job Practice" section in this manual.

ISACA created this publication as an educational resource to assist individuals who are preparing to take the CISA exam. It was produced independently from the CISA Certification Working Group, which has no responsibility for its content. Copies of past exams are not released to the public and are not made available to candidates. ISACA makes no representations or warranties whatsoever regarding these or other ISACA or IT Governance Institute publications assuring candidates' passage of the CISA exam.

ISACA wishes you success with the CISA exam. Your commitment to pursuing the leading certification for information systems (IS) audit, assurance, security and control professionals is exemplary, and ISACA welcomes your comments and suggestions on the use and coverage of this manual. After completion of the exam, please complete the online evaluation that corresponds to this publication *(www.isaca.org/studyaidsevaluation)*. Your observations will be invaluable as new questions, answers and explanations are prepared.

ACKNOWLEDGMENTS

This CISA® Review Questions, Answers & Explanations Manual 12th Edition is the result of the collective efforts of many volunteers. ISACA members from throughout the world participated, generously offering their talents and expertise. This international team exhibited a spirit and selflessness that has become the hallmark of contributors to this valuable manual. Their participation and insight are truly appreciated.

NEW–CISA JOB PRACTICE

Beginning in 2019, the Certified Information Systems Auditor (CISA) exam tests the new CISA job practice.

An international job practice analysis is conducted periodically to maintain the validity of the CISA certification program. A new job practice forms the basis of the CISA exam.

The primary focus of the job practice is on the current tasks performed and the knowledge used by CISAs. By gathering evidence of the current work practice of CISAs, ISACA ensures that the CISA program continues to meet the high standards for the certification of professionals throughout the world.

The findings of the CISA job practice analysis are carefully considered and directly influence the development of new test specifications to ensure that the CISA exam reflects the most current best practices.

The new job practice reflects the areas of study to be tested and is compared below to the previous job practice. The complete CISA job practice is at *www.isaca.org/cisajobpractice*.

Previous CISA Job Practice	New CISA Job Practice
Domain 1: The Process of Auditing Information Systems (21%)	**Domain 1: Information System Auditing Process (21%)**
Domain 2: Governance and Management of IT (16%)	**Domain 2: Governance and Management of IT (17%)**
Domain 3: Information Systems Acquisition, Development and Implementation (18%)	**Domain 3: Information Systems Acquisition, Development and Implementation (12%)**
Domain 4: Information Systems Operations, Maintenance and Service Management (20%)	**Domain 4: Information Systems Operations and Business Resilience (23%)**
Domain 5: Protection of Information Assets (25%)	**Domain 5: Protection of Information Assets (27%)**

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

Each CISA question has a stem (question) and four options (answer choices). The candidate is asked to choose the best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description of a problem may be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided.

When candidates prepare for the exam, they should recognize that IS audit and control is a global profession, and individual perceptions and experiences may not reflect the more global position or circumstance. Because the exam and CISA manuals are written for the international IS audit and control community, a candidate will be required to be somewhat flexible when reading an audit or control condition that may be contrary to a candidate's experience. It should be noted that CISA exam questions are written by experienced IS audit practitioners from around the world. Each question on the exam is reviewed by ISACA's CISA Test Enhancement Subcommittee and CISA Certification Working Group, which consist of international members. This geographical representation ensures that all test questions are understood equally in each country and language.

Note: ISACA review manuals are living documents. As technology advances, ISACA manuals are updated to reflect such advances. Further updates to this document before the date of the exam can be viewed at *www.isaca.org/studyaidupdates*.

Any suggestions to enhance the materials covered herein, or reference materials, should be submitted online at *support.isaca.org*.

INTRODUCTION

OVERVIEW

This manual consists of 1,000 multiple-choice questions, answers and explanations. The questions are numbered **A1-1**, **A2-1**, etc.

Questions Sorted by Domain
Questions, answers and explanations are sorted by the CISA job practice domains. The CISA candidate can refer to specific domain questions to evaluate comprehension of the topics that are covered within each domain. These questions are representative of CISA exam questions, although they are not actual exam items. The questions assist the CISA candidate in understanding the materials in the *CISA® Review Manual 27th Edition* and depict the type of question format typically found on the CISA exam. The number of questions, answers and explanations provided in the five domain sections in this publication provide the CISA candidate with the maximum number of study questions.

Sample Exam
A sample exam of 150 questions is also provided in this manual. **This exam is organized according to the domain percentages specified in the CISA job practice and used on the CISA exam:**
- Domain 1—Information System Auditing Process.....21 percent
- Domain 2—Governance and Management of IT.....17 percent
- Domain 3—Information Systems Acquisition, Development and Implementation.....12 percent
- Domain 4—Information Systems Operations and Business Resilience.....23 percent
- Domain 5—Protection of Information Assets.....27 percent

Candidates are urged to use this sample exam and the answer sheet provided to simulate an actual exam. Many candidates use this exam as a pretest to determine their strengths or weaknesses, or as a final exam. The sample exam answer sheet is provided for both uses. In addition, a CISA sample exam answer and reference key is included that cross references the exam questions to the questions in this publication, so it is convenient to refer to the explanations of the correct answers. This publication is ideal to use with the *CISA® Review Manual 27th Edition*.

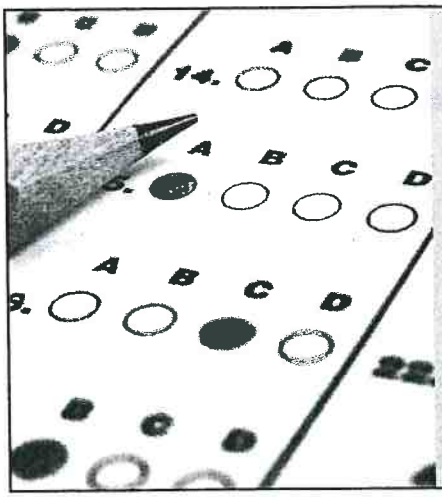
The *CISA® Review Questions, Answers & Explanations Manual 12th Edition* was developed to assist CISA candidates in studying and preparing for the CISA exam. As candidates use this publication to prepare for the exam, they should note that it covers a broad spectrum of IS audit, assurance, control and security issues. Candidates should not assume that reading and working through the questions in this manual will fully prepare them for the exam. Because exam questions often relate to practical experiences, CISA candidates are cautioned to refer to their own experiences and to other publications referred to in the *CISA® Review Manual 27th Edition*. These additional references are excellent sources of further detailed information and clarification. It is recommended that candidates evaluate the job practice domains in which they feel weak or require a further understanding, and study accordingly.

This publication uses standard American English.

TYPES OF QUESTIONS ON THE CISA EXAM

CISA exam questions are developed with the intent of measuring and testing practical knowledge and applying general concepts and standards. Questions are presented in a multiple-choice format and are designed for one best answer.

The candidate is cautioned to read each question carefully. Many times, a CISA exam question will require the candidate to choose the appropriate answer that is most likely or best or choose a practice or procedure that would be performed first, related to the other answers. In every case, the candidate is required to read the question carefully, eliminate known wrong answers and then make the best choice possible. Knowing that these types of questions are asked and how to study to answer them will help candidates to answer these types of questions correctly.



PRETEST

If you wish to take a pretest to determine strengths and weaknesses, the Sample Exam begins on page 469 and the pretest answer sheet begins on page 493. You can score your pretest with the Sample Exam Answer and Reference Key on page 491.

Page intentionally left blank

QUESTIONS, ANSWERS & EXPLANATIONS BY DOMAIN

DOMAIN 1—INFORMATION SYSTEM AUDITING PROCESS (21%)

A1-1 The internal audit department wrote some scripts that are used for continuous auditing of some information systems. The IT department asked for copies of the scripts so that they can use them for setting up a continuous monitoring process on key systems. Does sharing these scripts with IT affect the ability of the IS auditors to independently and objectively audit the IT function?

A. Sharing the scripts is not permitted because it gives IT the ability to pre-audit systems and avoid an accurate, comprehensive audit.
B. Sharing the scripts is required because IT must have the ability to review all programs and software that run on IS systems regardless of audit independence.
C. Sharing the scripts is permissible if IT recognizes that audits may still be conducted in areas not covered in the scripts.
D. Sharing the scripts is not permitted because the IS auditors who wrote the scripts would not be permitted to audit any IS systems where the scripts are being used for monitoring.

C is the correct answer.

Justification:
A. The ability of IT to continuously monitor and address any issues on IT systems does not affect the ability of IS audit to perform a comprehensive audit.
B. Sharing the scripts may be required by policy for quality assurance and configuration management, but that does not impair the ability to audit.
C. **IS audit can still review all aspects of the systems. They may not be able to review the effectiveness of the scripts, but they can still audit the systems.**
D. An audit of an IS system encompasses more than just the controls covered in the scripts.

A1-2 Which of the following is the **BEST** factor for determining the required extent of data collection during the planning phase of an IS compliance audit?

A. Complexity of the organization's operation
B. Findings and issues noted from the prior year
C. Purpose, objective and scope of the audit
D. Auditor's familiarity with the organization

C is the correct answer.

Justification:
A. The complexity of the organization's operation is a factor in the planning of an audit but does not directly affect the determination of how much data to collect. The extent of data collection is subject to the intensity, scope and purpose of the audit.
B. Prior findings and issues are factors in the planning of an audit but do not directly affect the determination of how much data to collect. Data must be collected outside of areas of previous findings.
C. **The extent to which data will be collected during an IS audit is related directly to the purpose, objective and scope of the audit. An audit with a narrow purpose and limited objective and scope is most likely to result in less data collection than an audit with a wider purpose and scope. Statistical analysis may also determine the extent of data collection, such as sample size or means of data collection.**
D. An auditor's familiarity with the organization is a factor in the planning of an audit but does not directly affect the determination of how much data to collect. The audit must be based on sufficient evidence of the monitoring of controls and not unduly influenced by the auditor's familiarity with the organization.

A1-3 An IS auditor is developing an audit plan for an environment that includes new systems. The organization's management wants the IS auditor to focus on recently implemented systems. How should the IS auditor respond?

A. Audit the new systems as requested by management.
B. Audit systems not included in last year's scope.
C. Determine the highest-risk systems and plan accordingly.
D. Audit both the systems not in last year's scope and the new systems.

C is the correct answer.

Justification:

A. Auditing the new system does not reflect a risk-based approach. Although the system can contain sensitive data and may present risk of data loss or disclosure to the organization, without a risk assessment, the decision to solely audit the newly implemented system is not a risk-based decision.
B. Auditing systems not included in the previous year's scope does not reflect a risk-based approach. In addition, management may know about problems with the new system and may be intentionally trying to steer the audit away from that vulnerable area. Although, at first, the new system may seem to be the riskiest area, an assessment must be conducted rather than relying on the judgment of the IS auditor or IT manager.
C. **The best action is to conduct a risk assessment and design the audit plan to cover the areas of highest risk. ISACA IS Audit and Assurance Standard 1202 (Risk Assessment in Planning), statement 1202.1: "The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources."**
D. The creation of the audit plan should be performed in cooperation with management and based on risk. The IS auditor should not arbitrarily decide on what needs to be audited.

A1-4 An IS auditor is reviewing security controls for a critical web-based system prior to implementation. The results of the penetration test are inconclusive, and the results will not be finalized prior to implementation. Which of the following is the **BEST** option for the IS auditor?

A. Publish a report based on the available information, highlighting the potential security weaknesses and the requirement for follow-up audit testing.
B. Publish a report omitting the areas where the evidence obtained from testing was inconclusive.
C. Request a delay of the implementation date until additional security testing can be completed and evidence of appropriate controls can be obtained.
D. Inform management that audit work cannot be completed prior to implementation and recommend that the audit be postponed.

A is the correct answer.

Justification:

A. **If the IS auditor cannot gain sufficient assurance for a critical system within the agreed-on time frame, this fact should be highlighted in the audit report and follow-up testing should be scheduled for a later date. Management can then determine whether any of the potential weaknesses identified were significant enough to delay the go-live date for the system.**
B. It is not acceptable for the IS auditor to ignore areas of potential weakness because conclusive evidence could not be obtained within the agreed-on audit time frame. ISACA IS Audit and Assurance Standards are violated if these areas are omitted from the audit report.
C. Extending the time frame for the audit and delaying the go-live date is unlikely to be acceptable in this scenario where the system involved is business-critical. In any case, a delay to the go-live date must be the decision of business management, not the IS auditor. In this scenario, the IS auditor should present business management with all available information by the agreed-on date.
D. Failure to obtain sufficient evidence in one part of an audit engagement does not justify cancelling or postponing the audit; this violates the audit guideline concerning due professional care.

A1-5 Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls

D is the correct answer.

Justification:

A. Overlapping controls are two controls addressing the same control objective or exposure. Because primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls.
B. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself and are individual-based, not role-based, controls.
C. Access controls for resources are based on individuals and not on roles. For a lack of segregation of duties, the IS auditor expects to find that a person has higher levels of access than are ideal. The IS auditor wants to find compensating controls to address this risk.
D. Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated.

A1-6 Which of the following is the key benefit of a control self-assessment?

A. Management ownership of the internal controls supporting business objectives is reinforced.
B. Audit expenses are reduced when the assessment results are an input to external audit work.
C. Fraud detection is improved because internal business staff are engaged in testing controls.
D. Internal auditors can shift to a consultative approach by using the results of the assessment.

A is the correct answer.

Justification:

A. The objective of control self-assessment (CSA) is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance.
B. Reducing audit expenses is not a key benefit of CSA.
C. Improved fraud detection is important but not as important as control ownership. It is not a principal objective of CSA.
D. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

A1-7 What is the **PRIMARY** requirement that a data mining and auditing software tool should meet? The software tool should:

A. interface with various types of enterprise resource planning software and databases.
B. accurately capture data from the organization's systems without causing excessive performance problems.
C. introduce audit hooks into the organization's financial systems to support continuous auditing.
D. be customizable and support inclusion of custom programming to aid in investigative analysis.

B is the correct answer.

Justification:
A. The product must interface with the types of systems used by the organization and provide meaningful data for analysis.
B. Although all the requirements that are listed as answer choices are desirable in a software tool evaluated for auditing and data mining purposes, the most critical requirement is that the tool works effectively on the systems of the organization being audited.
C. The tool should probably work on more than just financial systems and does not necessarily require implementation of audit hooks.
D. The tool should be flexible but not necessarily customizable. It should have built-in analysis software tools.

A1-8 A long-term IT employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be **PRIMARILY** based on the individual's experience and:

A. length of service, because this will help ensure technical competence.
B. age, because training in audit techniques may be impractical.
C. IT knowledge, because this will bring enhanced credibility to the audit function.
D. ability, as an IS auditor, to be independent of existing IT relationships.

D is the correct answer.

Justification:
A. Length of service does not ensure technical competency.
B. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.
C. The fact that the employee has worked in IT for many years may not ensure credibility. The IS audit department's needs should be defined, and any candidate should be evaluated against those requirements.
D. Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities.

A1-9 For a retail business with a large volume of transactions, which of the following audit techniques is the **MOST** appropriate for addressing emerging risk?

A. Use of computer-assisted audit techniques
B. Quarterly risk assessments
C. Sampling of transaction logs
D. Continuous auditing

D is the correct answer.

Justification:

A. Using software tools such as computer-assisted audit techniques to analyze transaction data can provide detailed analysis of trends and potential risk, but it is not as effective as continuous auditing, because there may be a time differential between executing the software and analyzing the results.
B. Quarterly risk assessment may be a good technique but not as responsive as continuous auditing.
C. The sampling of transaction logs is a valid audit technique; however, risk may exist that is not captured in the transaction log, and there may be a potential time lag in the analysis.
D. The implementation of continuous auditing enables a real-time feed of information to management through automated reporting processes so that management may implement corrective actions more quickly.

A1-10 An IS auditor is reviewing access to an application to determine whether recently added accounts were appropriately authorized. This is an example of:

A. variable sampling.
B. substantive testing.
C. compliance testing.
D. stop-or-go sampling.

C is the correct answer.

Justification:

A. Variable sampling is used to estimate numerical values such as dollar values.
B. Substantive testing substantiates the integrity of actual processing such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized.
C. Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized.
D. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

A1-11 The decisions and actions of an IS auditor are **MOST** likely to affect which of the following types of risk?

A. Inherent
B. Detection
C. Control
D. Business

B is the correct answer.

Justification:

A. Inherent risk is the risk that a material error could occur, if there are no related internal controls to prevent or detect the error. Inherent risk is not usually affected by an IS auditor.
B. Detection risk is directly affected by the IS auditor's selection of audit procedures and techniques. Detection risk is the risk that a review will not detect or notice a material issue.
C. Control risk is the risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls. Control risk can be mitigated by the actions of the organization's management.
D. Business risk is a probable situation with uncertain frequency and magnitude of loss (or gain). Business risk is usually not directly affected by an IS auditor.

A1-12 Which of the following is the **MOST** critical step when planning an IS audit?

A. Review findings from prior audits
B. Executive management's approval of the audit plan
C. Review information security policies and procedures
D. Perform a risk assessment

D is the correct answer.

Justification:

A. The findings of a previous audit are of interest to the auditor, but they are not the most critical step. The most critical step involves finding the current issues or high-risk areas, not reviewing the resolution of older issues. A review of historical audit findings could indicate that management is not resolving the items or the recommendation was ineffective.
B. Executive management is not required to approve the audit plan. It is typically approved by the audit committee or board of directors. Management could recommend areas to audit.
C. Reviewing information security policies and procedures is normally be conducted during fieldwork, not planning.
D. Of all the steps listed, performing a risk assessment is the most critical. Risk assessment is required by ISACA IS Audit and Assurance Standard 1202 (Risk Assessment in Planning), statement 1202.2: "IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements." In addition to the standards requirement, if a risk assessment is not performed, then high-risk areas of the auditee systems or operations may not be identified for evaluation.

A1-13 An IS auditor is reviewing a software application that is built on the principles of service-oriented architecture. What is the **INITIAL** step?

A. Understanding services and their allocation to business processes by reviewing the service repository documentation.
B. Sampling the use of service security standards as represented by the Security Assertions Markup Language.
C. Reviewing the service level agreements established for all system providers.
D. Auditing the core service and its dependencies on other systems.

A is the correct answer.

Justification:

A. **A service-oriented architecture relies on the principles of a distributed environment in which services encapsulate business logic as a black box and might be deliberately combined to depict real-world business processes. Before reviewing services in detail, it is essential for the IS auditor to comprehend the mapping of business processes to services.**
B. Sampling the use of service security standards as represented by the Security Assertions Markup Language is an essential follow-up step to understanding services and their allocation to business but is not the initial step.
C. Reviewing the service level agreements is an essential follow-up step to understanding services and their allocation to business but is not the initial step.
D. Auditing the core service and its dependencies with others would most likely be a part of the audit, but the IS auditor must first gain an understanding of the business processes and how the systems support those processes.

A1-14 An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Delete all copies of the unauthorized software.
B. Recommend an automated process to monitor for compliance with software licensing.
C. Report the use of the unauthorized software and the need to prevent recurrence.
D. Warn the end users about the risk of using illegal software.

C is the correct answer.

Justification:

A. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing the unauthorized software.
B. This would detect compliance with software licensing. However, an automated solution might not be the best option in all cases.
C. **The use of unauthorized or illegal software should be prohibited by an organization. An IS auditor must convince the user and management of the risk and the need to eliminate the risk. For example, software piracy can result in exposure and severe fines.**
D. Auditors must report material findings to management for action. Informing the users of risk is not the primary responsibility of the IS auditor.

A1-15 An audit charter should:

A. be dynamic and change to coincide with the changing nature of technology and the audit profession.
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
C. document the audit procedures designed to achieve the planned audit objectives.
D. outline the overall authority, scope and responsibilities of the audit function.

D is the correct answer.

Justification:

A. The audit charter should not be subject to changes in technology and should not significantly change over time. The charter should be approved at the highest level of management.
B. An audit charter states the authority and reporting requirements for the audit but not the details of maintenance of internal controls.
C. An audit charter is not at a detailed level and, therefore, does not include specific audit objectives or procedures.
D. An audit charter should state management's objectives for and delegation of authority to IS auditors.

A1-16 An IS auditor finds a small number of user access requests that were not authorized by managers through the normal predefined workflow steps and escalation rules. The IS auditor should:

A. perform an additional analysis.
B. report the problem to the audit committee.
C. conduct a security risk assessment.
D. recommend that the owner of the identity management system fix the workflow issues.

A is the correct answer.

Justification:

A. The IS auditor needs to perform substantive testing and additional analysis to determine why the approval and workflow processes are not working as intended. Before making any recommendation, the IS auditor should gain a good understanding of the scope of the problem and the factors that caused this incident. The IS auditor should identify whether the issue was caused by managers not following procedures, a problem with the workflow of the automated system or a combination of the two.
B. The IS auditor does not yet have enough information to report the problem.
C. Changing the scope of the IS audit or conducting a security risk assessment requires more detailed information about the processes and violations being reviewed.
D. The IS auditor must first determine the root cause and impact of the findings and does not have enough information to recommend fixing the workflow issues.

A1-17 Which of the following sampling methods is **MOST** useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean-per-unit sampling
D. Difference estimation sampling

A is the correct answer.

Justification:

A. **Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. For example, an attribute sample may check all transactions over a certain predefined dollar amount for proper approvals.**
B. Variable sampling is based on the calculation of a mean from a sample extracted from the entire population and using that to estimate the characteristics of the entire population. For example, a sample of 10 items shows an average price of US $10 per item. For the entire population of 1,000 items, the total value is estimated to be US $10,000. This is not a good way to measure compliance with a process.
C. Stratified mean sampling attempts to ensure that the entire population is represented in the sample. This is not an effective way to measure compliance.
D. Difference estimation sampling examines measure deviations and extraordinary items and is not a good way to measure compliance.

A1-18 When testing program change requests for a remote system, an IS auditor finds that the number of changes available for sampling does not provide a reasonable level of assurance. What is the **MOST** appropriate action for the IS auditor to take?

A. Develop an alternate testing procedure.
B. Report the finding to management.
C. Perform a walkthrough of the change management process.
D. Create additional sample data to test additional changes.

A is the correct answer.

Justification:

A. **If a sample-size objective cannot be met with the given data, the IS auditor cannot provide assurance regarding the testing objective. In this instance, the IS auditor should develop (with audit management approval) an alternate testing procedure.**
B. There is not enough evidence to report the finding as a deficiency.
C. A walkthrough should not be initiated until an analysis is performed to confirm that this could provide the required assurance.
D. It is not appropriate for an IS auditor to create sample data for the purpose of the audit.

A1-19 Which of the following situations could impair the independence of an IS auditor? The IS auditor:

A. implemented specific functionality during the development of an application.
B. designed an embedded audit module for auditing an application.
C. participated as a member of an application project team and did not have operational responsibilities.
D. provided consulting advice concerning application good practices.

A is the correct answer.

Justification:

A. Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system.
B. Designing an embedded audit module does not impair an IS auditor's independence.
C. IS auditors should not audit work that they have done, but just participating as a member of the application system project team does not impair an IS auditor's independence.
D. An IS auditor's independence is not impaired by providing advice on known good practices.

A1-20 The **PRIMARY** advantage of a continuous audit approach is that it:

A. does not require an IS auditor to collect evidence on system reliability while processing is taking place.
B. allows the IS auditor to review and follow up on audit issues in a timely manner.
C. places the responsibility for enforcement and monitoring of controls on the security department instead of audit.
D. simplifies the extraction and correlation of data from multiple and complex systems.

B is the correct answer.

Justification:

A. The continuous audit approach often requires an IS auditor to collect evidence on system reliability while processing is taking place.
B. Continuous audit allows audit and response to audit issues in a timely manner because audit findings are gathered in near real time.
C. Responsibility for enforcement and monitoring of controls is primarily the responsibility of management.
D. The use of continuous audit is not based on the complexity or number of systems being monitored.

A1-21 Which of the following would impair the independence of a quality assurance team?

A. Ensuring compliance with development methods
B. Checking the test assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation

C is the correct answer.

Justification:

A. Ensuring compliance with development methods is a valid quality assurance function.
B. Checking the test assumptions is a valid quality assurance function.
C. Correction of code should not be a responsibility of the quality assurance team, because it would not ensure segregation of duties and would impair the team's independence.
D. Checking the code to ensure proper documentation is a valid quality assurance function.

A1-22 In planning an IS audit, the **MOST** critical step is the identification of the:

A. areas of significant risk
B. skill sets of the audit staff
C. test steps in the audit
D. time allotted for the audit

A is the correct answer.

Justification:

A. **When designing a risk-based audit plan, it is important to identify the areas of highest risk to determine the areas to be audited.**
B. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Where the skills are inadequate, the organization should consider using external resources.
C. Test steps for the audit are not as critical during the audit planning process as identifying the areas of risk that should be audited.
D. The time allotted for an audit is determined during the planning process based on the areas to be audited and is primarily based on the requirement for conducting an appropriate audit.

A1-23 The **MOST** effective audit practice to determine whether the operational effectiveness of controls is properly applied to transaction processing is:

A. control design testing.
B. substantive testing.
C. inspection of relevant documentation.
D. perform tests on risk prevention.

B is the correct answer.

Justification:

A. Testing of control design assesses whether the control is structured to meet a specific control objective. It does not help determine whether the control is operating effectively.
B. **Among other methods, such as document review or walkthrough, tests of controls are the most effective procedures to assess whether controls accurately support operational effectiveness.**
C. Control documents may not always describe the actual process in an accurate manner. Therefore, auditors relying on document review have limited assurance that the control is operating as intended.
D. Performing tests on risk prevention is considered compliance testing. This type of testing is used to determine whether policies are adhered to.

A1-24 The extent to which data will be collected during an IS audit should be determined based on the:

A. Availability of critical and required information.
B. Auditor's familiarity with the circumstances.
C. Auditee's ability to find relevant evidence.
D. Purpose and scope of the audit being done.

D is the correct answer.

Justification:

A. The extent to which data will be collected during an IS audit should be based on the scope, purpose and requirements of the audit and not be constrained by the ease of obtaining the information or by the IS auditor's familiarity with the area being audited.
B. An IS auditor must be objective and thorough and not subject to audit risk through preconceived expected results based on familiarity with the area being audited.
C. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence. If evidence is not readily available, the auditor must ensure that other forms of audit are considered to ensure compliance in the area that is subject to audit.
D. The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An IS audit with a narrow purpose and scope, or just a high-level review, will most likely require less data collection than an audit with a wider purpose and scope.

A1-25 While planning an IS audit, an assessment of risk should be made to provide:

A. reasonable assurance that the audit will cover material items.
B. definite assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered by the audit.
D. sufficient assurance that all items will be covered during the audit work.

A is the correct answer.

Justification:

A. ISACA IS Audit and Assurance Guideline 2202 (Risk Assessment and Audit Planning) states that the applied risk assessment approach should help with the prioritization and scheduling process of the IS audit and assurance work. The risk assessment should support the selection process of areas and items of audit interest and the decision process to design and conduct particular IS audit engagements.
B. Definite assurance that material items will be covered during the audit work is an impractical proposition.
C. Reasonable assurance that all items will be covered during the audit work is not the correct answer, because primarily material items need to be covered, not all items.
D. Sufficient assurance that all items will be covered is not as important as ensuring that the audit will cover all material items.

A1-26 The **MOST** appropriate action for an IS auditor to take when shared user accounts are discovered is to:

A. inform the audit committee of the potential issue.
B. review audit logs for the IDs in question.
C. document the finding and explain the risk of using shared IDs.
D. request that the IDs be removed from the system.

C is the correct answer.

Justification:
A. It is not appropriate for an IS auditor to report findings to the audit committee before conducting a more detailed review and presenting them to management for a response.
B. Review of audit logs would not be useful because shared IDs do not provide for individual accountability.
C. An IS auditor's role is to detect and document findings and control deficiencies. Part of the audit report is to explain the reasoning behind the findings. The use of shared IDs is not recommended because it does not allow for accountability of transactions. An IS auditor defers to management to decide how to respond to the findings presented.
D. It is not the role of an IS auditor to request the removal of IDs from the system.

A1-27 An IS auditor is conducting a compliance test to determine whether controls support management policies and procedures. The test will assist the IS auditor to determine:

A. that the control is operating efficiently.
B. that the control is operating as designed.
C. the integrity of data controls.
D. the reasonableness of financial reporting controls.

B is the correct answer.

Justification:
A. It is important that controls operate efficiently, but in this case the intent is to ensure that the controls support management policies and procedures. Therefore, the important issue is whether the controls are operating correctly and thereby meeting the control objective.
B. Compliance tests can be used to test the existence and effectiveness of a defined process. Understanding the objective of a compliance test is important. IS auditors want reasonable assurance that the controls they are relying on are effective. An effective control is one that meets management expectations and objectives.
C. Substantive tests, not compliance tests, are associated with data integrity.
D. Determining the reasonableness of financial reporting controls is a very narrow answer in that it is limited to financial reporting. It meets the objective of determining whether the controls are reasonable but does not ensure that the control is working correctly and thereby supporting management expectations and objectives.

A1-28 The vice president of human resources has requested an IS audit to identify payroll overpayments for the previous year. Which would be the **BEST** audit technique to use in this situation?

A. Generate sample test data
B. Generalized audit software
C. Integrated test facility
D. Embedded audit module

B is the correct answer.

Justification:

A. Test data tests for the existence of controls that might prevent overpayments, but it does not detect specific, previous miscalculations.
B. Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and re-computations. An IS auditor, using generalized audit software, can design appropriate tests to recompute the payroll, thereby determining whether there were overpayments and to whom they were made.
C. An integrated test facility helps to identify a problem as it occurs but does not detect errors for a previous period.
D. An embedded audit module can enable the IS auditor to evaluate a process and gather audit evidence, but it does not detect errors for a previous period.

A1-29 During a security audit of IT processes, an IS auditor finds that documented security procedures do not exist. The IS auditor should:

A. Create the procedures document based on the practices.
B. Issue an opinion of the current state and end the audit.
C. Conduct compliance testing on available data.
D. Identify and evaluate existing practices.

D is the correct answer.

Justification:

A. IS auditors should not prepare documentation because the process may not be compliant with management objectives and doing so could jeopardize their independence.
B. Ending the audit and issuing an opinion will not address identification of potential risk. The auditor should evaluate the practices in place. The recommendation may still be for the organization to develop written procedures. Terminating the audit may prevent achieving one of the basic audit objectives—identification of potential risk.
C. Because there are no documented procedures, there is no basis against which to test compliance.
D. One of the main objectives of an audit is to identify potential risk; therefore, the most proactive approach is to identify and evaluate the existing security practices being followed by the organization and submit the findings and risk to management, with recommendations to document the current controls or enforce the documented procedures.

A1-30 During a risk analysis, an IS auditor identifies threats and potential impacts. Next, the IS auditor should:

A. Ensure the risk assessment is aligned to management's risk assessment process.
B. Identify information assets and the underlying systems.
C. Disclose the threats and impacts to management.
D. Identify and evaluate the existing controls.

D is the correct answer.

Justification:
A. An audit risk assessment is conducted for purposes that are different from management's risk assessment process purposes.
B. It is impossible to determine impact without first identifying the assets affected; therefore, this must already have been completed.
C. Upon completion of a risk assessment, an IS auditor should describe and discuss with management the threats and potential impacts on the assets, and recommendations for addressing the risk. However, this action cannot be done until the controls are identified and the likelihood of the threat is calculated.
D. It is important for an IS auditor to identify and evaluate the existence and effectiveness of existing and planned controls so that the risk level can be calculated after the potential threats and possible impacts are identified.

A1-31 Which of the following would normally be the **MOST** reliable evidence for an IS auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed
C. Trend data obtained from Internet sources
D. Ratio analysis developed by the IS auditor from reports supplied by line management

A is the correct answer.

Justification:
A. Evidence obtained from independent third parties is almost always considered to be more reliable than assurance provided by local management.
B. Because management is not objective and may not understand the risk and control environment, and they are only providing evidence that the application is working correctly (not the controls), their assurance is not an acceptable level of trust for audit evidence.
C. Data collected from the Internet is not always trustworthy or independently validated.
D. Ratio analysis can identify trends and deviations from a baseline but is not reliable evidence.

A1-32 When evaluating the collective effect of preventive, detective and corrective controls within a process, an IS auditor should be aware of which of the following?

A. The point at which controls are exercised as data flow through the system.
B. Only preventive and detective controls are relevant.
C. Corrective controls are regarded as compensating.
D. Classification allows an IS auditor to determine the controls that are missing.

A is the correct answer.

Justification:
A. An IS auditor should focus on when controls are exercised as data flow through a computer system.
B. Corrective controls may also be relevant because they allow an error or problem to be corrected.
C. Corrective controls remove or reduce the effects of errors or irregularities and are not exclusively regarded as compensating controls.
D. The existence and function of controls are important but not the classification.

A1-33 Which audit technique provides the **BEST** evidence of the segregation of duties in an IT department?

A. Discussion with management
B. Review of the organization chart
C. Observation and interviews
D. Testing of user access rights

C is the correct answer.

Justification:

A. Management may not be aware of the detailed functions of each employee in the IT department and whether the controls are being followed. Therefore, discussion with the management provides only limited information regarding segregation of duties.
B. An organization chart does not provide details of the functions of the employees or whether the controls are working correctly.
C. **Based on the observations and interviews, the IS auditor can evaluate the segregation of duties. By observing the IT staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations. By interviewing the IT staff, the auditor can get an overview of the tasks performed.**
D. Testing of user rights provides information about the rights users have within the IS systems but does not provide complete information about the functions they perform. Observation is a better option because user rights can be changed between audits.

A1-34 After reviewing the disaster recovery planning process of an organization, an IS auditor requests a meeting with organization management to discuss the findings. Which of the following **BEST** describes the main goal of this meeting?

A. Obtain management approval of the corrective action plan.
B. Confirm factual accuracy of the findings.
C. Assist management in the implementation of corrective actions.
D. Prioritize the resolution of the items.

B is the correct answer.

Justification:

A. Management approval of the corrective action plan is not required. Management can elect to implement another corrective action plan to address the risk.
B. **The goal of the meeting is to confirm the factual accuracy of the audit findings and present an opportunity for management to agree on or respond to recommendations for corrective action.**
C. Implementation of corrective actions should be done after the factual accuracy of findings is established, but the work of implementing corrective action is not typically assigned to the IS auditor, because this impairs the auditor's independence.
D. Rating the audit findings provides guidance to management for allocating resources to the high-risk items first.

A1-35 An IS auditor should ensure that review of online electronic funds transfer reconciliation procedures include:

A. Vouching.
B. Authorizations.
C. Corrections.
D. Tracing.

D is the correct answer.

Justification:

A. Vouching is usually performed during the funds transfer, not during the reconciliation effort.
B. In online processing, authorizations are normally done automatically by the system, not during the reconciliation.
C. Correction entries should be reviewed during a reconciliation; however, they are normally done by an individual other than the person entrusted to do reconciliations and are not as important as tracing.
D. Tracing is a transaction reconciliation effort that involves following the transaction from the original source to its final destination. In electronic funds transfer transactions, the direction on tracing may start from the customer-printed copy of the receipt, proceed to checking the system audit trails and logs, and end with checking the master file records for daily transactions.

A1-36 An IS auditor is carrying out a system configuration review. Which of the following is the **BEST** evidence in support of the current system configuration settings?

A. System configuration values that are imported to a spreadsheet by the system administrator
B. Standard report with configuration values that are retrieved from the system by the IS auditor
C. Dated screenshot of the system configuration settings that are made available by the system administrator
D. Annual review of approved system configuration values by the business owner

B is the correct answer.

Justification:

A. Evidence that is not system-generated information can be modified before it is presented to an IS auditor. Therefore, it may not be as reliable as evidence that is obtained by the IS auditor. For example, a system administrator can change the settings or modify the graphic image before taking a screenshot.
B. Evidence that is obtained directly from the source by an IS auditor is more reliable than information that is provided by a system administrator or a business owner, because the IS auditor does not have a vested interest in the outcome of the audit.
C. The rules may be modified by the administrator prior to taking the screenshot; therefore, this is not the best evidence.
D. The annual review provided by a business owner may not reflect current information.

A1-37 The purpose of a checksum on an amount field in an electronic data interchange communication of financial transactions is to ensure:

A. Integrity.
B. Authenticity.
C. Authorization.
D. Nonrepudiation.

A is the correct answer.

Justification:

A. A checksum that is calculated on an amount field and included in the electronic data interchange communication can be used to identify unauthorized modifications.
B. Authenticity cannot be established by a checksum alone and needs other controls.
C. Authorization cannot be established by a checksum alone and needs other controls.
D. Nonrepudiation can be ensured by using digital signatures.

A1-38 Which of the following forms of evidence would an IS auditor consider the **MOST** reliable?

A. An oral statement from the auditee
B. The results of a test that is performed by an external IS auditor
C. An internally generated computer accounting report
D. A confirmation letter that is received from an outside source

B is the correct answer.

Justification:

A. An oral statement from the auditee is audit evidence but not as reliable as the results of a test that is performed by an external IS auditor.
B. An independent test that is performed by an IS auditor should always be considered a more reliable source of evidence than a confirmation letter from a third party, because the letter is the result of an analysis of the process and may not be based on authoritative audit techniques. An audit should consist of a combination of inspection, observation and inquiry by an IS auditor as determined by risk. This provides a standard methodology and reasonable assurance that the controls and test results are accurate.
C. An internally generated computer accounting report is audit evidence, but is not as reliable as the results of a test performed by an external IS auditor.
D. An independent test performed by an IS auditor should always be considered a more reliable source of evidence than a confirmation letter from a third party, because a letter is subjective and may not have been generated as a part of an authoritative audit or conform to audit standards.

A1-39 An IS auditor who has discovered unauthorized transactions during a review of electronic data interchange (EDI) transactions is likely to recommend improving the:

A. EDI trading partner agreements.
B. Physical controls for terminals.
C. Authentication techniques for sending and receiving messages.
D. Program change control procedures.

C is the correct answer.

Justification:
A. The electronic data interchange trading partner agreements minimize exposure to legal issues but do not resolve the problem of unauthorized transactions.
B. Physical control is important and may provide protection from unauthorized people accessing the system but does not provide protection from unauthorized transactions by authorized users.
C. **Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions.**
D. Change control procedures do not resolve the issue of unauthorized transactions.

A1-40 An IS auditor is validating a control that involves a review of system-generated exception reports. Which of the following is the **BEST** evidence of the effectiveness of the control?

A. Walk-through with the reviewer of the operation of the control
B. System-generated exception reports for the review period with the reviewer's sign-off
C. A sample system-generated exception report for the review period, with follow-up action items noted by the reviewer
D. Management's confirmation of the effectiveness of the control for the review period

C is the correct answer.

Justification:
A. A walk-through highlights how a control is designed to work, but it seldom highlights the effectiveness of the control, or exceptions or constraints in the process.
B. Reviewer sign-off does not demonstrate the effectiveness of the control if the reviewer does not note follow-up actions for the exceptions identified.
C. **A sample of a system-generated report with evidence that the reviewer followed up on the exception represents the best possible evidence of the effective operation of the control, because there is documented evidence that the reviewer reviewed the exception report and took actions based on the exception report.**
D. Management's confirmation of effectiveness of the control suffers from lack of independence—management might be biased toward the effectiveness of the controls put in place.

A1-41 A company has recently upgraded its purchase system to incorporate electronic data interchange (EDI) transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgments

D is the correct answer.

Justification:
A. Key verification is used for encryption and protection of data but not for data mapping.
B. One-for-one checking validates that transactions are accurate and complete but does not map data.
C. Manual recalculations are used to verify that the processing is correct but do not map data.
D. Acting as an audit trail for electronic data interchange transactions, functional acknowledgments are one of the main controls used in data mapping.

A1-42 Which of the following sampling methods would be the **MOST** effective to determine whether purchase orders issued to vendors have been authorized as per the authorization matrix?

A. Variable sampling
B. Stratified mean per unit
C. Attribute sampling
D. Unstratified mean per unit

C is the correct answer.

Justification:
A. Variable sampling is the method used for substantive testing, which involves testing transactions for quantitative aspects such as monetary values.
B. Stratified mean per unit is used in variable sampling.
C. Attribute sampling is the method used for compliance testing. In this scenario, the operation of a control is being evaluated, and therefore, the attribute of whether each purchase order was correctly authorized would be used to determine compliance with the control.
D. Unstratified mean per unit is used in variable sampling.

A1-43 The **BEST** method of confirming the accuracy of a system tax calculation is by:

A. review and analysis of the source code of the calculation programs.
B. recreating program logic using generalized audit software to calculate monthly totals.
C. preparing simulated transactions for processing and comparing the results to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

C is the correct answer.

Justification:
A. A review of source code is not an effective method of ensuring that the calculation is being computed correctly.
B. Recreating program logic may lead to errors, and monthly totals are not accurate enough to ensure correct computations.
C. Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for confirming the accuracy of a tax calculation.
D. Flowcharting and analysis of source code are not effective methods to address the accuracy of individual tax calculations.

A1-44 An IS auditor performing a review of application controls would evaluate the:

A. efficiency of the application in meeting the business processes.
B. impact of any exposures discovered.
C. business processes served by the application.
D. application's optimization.

B is the correct answer.

Justification:

A. The IS auditor is reviewing the effectiveness of the controls, not the suitability of the application to meet business needs.
B. An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses.
C. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of the application controls.
D. One area to be reviewed may be the efficiency and optimization of the application, but this is not the area being reviewed in this audit.

A1-45 Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The IS auditor should:

A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
B. not include the finding in the final report because management resolved the item.
C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
D. include the finding in the closing meeting for discussion purposes only.

A is the correct answer.

Justification:

A. Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.
B. The audit report should contain all relevant findings and the response from management even if the finding has been resolved. This would mean that subsequent audits may test for the continued resolution of the control.
C. The audit report should contain the finding so that it is documented and the removal of the control subsequent to the audit would be noticed.
D. The audit report should contain the finding and resolution, and this can be mentioned in the final meeting. The audit report should list all relevant findings and the response from management.

A1-46 The internal IS audit team is auditing controls over sales returns and is concerned about fraud. Which of the following sampling methods will **BEST** assist the IS auditors?

A. Stop-or-go
B. Classical variable
C. Discovery
D. Probability-proportional-to-size

C is the correct answer.

Justification:

A. Stop-or-go is a sampling method that helps limit the size of a sample and allows the test to be stopped at the earliest possible moment.
B. Classical variable sampling is associated with dollar amounts and has a sample based on a representative sample of the population but is not focused on fraud.
C. Discovery sampling is used when an IS auditor is trying to determine whether a type of event has occurred. Therefore, it is suited to assess the risk of fraud and to identify whether a single occurrence has taken place.
D. Probability-proportional-to-size sampling is typically associated with cluster sampling when there are groups within a sample. The question does not indicate that an IS auditor is searching for a threshold of fraud.

A1-47 When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

A. Controls needed to mitigate risk are in place.
B. Vulnerabilities and threats are identified.
C. Audit risk is considered.
D. A gap analysis is appropriate.

B is the correct answer.

Justification:

A. Understanding whether appropriate controls that are required to mitigate risk are in place is a resultant effect of an audit.
B. While developing a risk-based audit strategy, it is critical that the risk and vulnerabilities are understood. They determine the areas to be audited and the extent of coverage.
C. Audit risk is an inherent aspect of auditing, directly related to the audit process and not relevant to the risk analysis of the environment to be audited.
D. A gap analysis is normally done to compare the actual state to an expected or desirable state.

A1-48 During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

A. Ask the auditee to sign a release form accepting full legal responsibility.
B. Elaborate on the significance of the finding and the risk of not correcting it.
C. Report the disagreement to the audit committee for resolution.
D. Accept the auditee's position because they are the process owners.

B is the correct answer.

Justification:

A. Management is always responsible and liable for risk. The role of the IS auditor is to inform management of the findings and associated risk discovered in an audit.
B. If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risk and exposures because the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee lessens effective communications and sets up an adversarial relationship, but an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.
C. The audit report contains the finding from the IS auditor and the response from management. It is the responsibility of management to accept risk or mitigate it appropriately. The role of the auditor is to inform management clearly and thoroughly so that the best decision can be made.
D. The IS auditor must be professional, competent and independent. They must not just accept an explanation or argument from management, unless the process used to generate the finding was flawed.

A1-49 To ensure that audit resources deliver the best value to the organization, the **FIRST** step in an audit project is to:

A. Schedule the audits and monitor the time spent on each audit.
B. Train the IS audit staff on current technology used in the organization.
C. Develop the audit plan based on a detailed risk assessment.
D. Monitor progress of audits and initiate cost control measures.

C is the correct answer.

Justification:

A. Monitoring the audits and the time spent on audits is not effective if the wrong areas are being audited. It is most important to develop a risk-based audit plan to ensure effective use of audit resources.
B. The IS auditor may have specialties, or the audit team may rely on outside experts to conduct very specialized audits. It is not necessary for each IS auditor to be trained on all new technology.
C. Although monitoring the time and audit programs, and adequate training improve the IS audit staff's productivity (efficiency and performance), ensuring that the resources and efforts being dedicated to audit are focused on higher-risk areas delivers value to the organization.
D. Monitoring audits and initiating cost controls does not ensure the effective use of audit resources.

A1-50 Which of the following should be the **FIRST** action of an IS auditor during a dispute with a department manager over audit findings?

A. Retest the control to validate the finding.
B. Engage a third party to validate the finding.
C. Include the finding in the report with the department manager's comments.
D. Revalidate the supporting evidence for the finding.

D is the correct answer.

Justification:

A. Retesting the control normally occurs after the evidence has been revalidated.
B. Although there are cases where a third party may be needed to perform specialized audit procedures, an IS auditor should first revalidate the supporting evidence to determine whether there is a need to engage a third party.
C. Before putting a disputed finding or management response in the audit report, the IS auditor should take care to review the evidence that is used in the finding to ensure audit accuracy.
D. Conclusions drawn by an IS auditor should be adequately supported by evidence, and any compensating controls or corrections that are pointed out by a department manager should be taken into consideration. Therefore, the first step is to revalidate the evidence for the finding. If, after revalidating and retesting, there are unsettled disagreements, those issues should be included in the report.

A1-51 An IS auditor should use statistical sampling, and not judgment (nonstatistical) sampling, when:

A. The probability of error must be objectively quantified.
B. The auditor wants to avoid sampling risk.
C. Generalized audit software is unavailable.
D. The tolerable error rate cannot be determined.

A is the correct answer.

Justification:

A. Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient).
B. Sampling risk is the risk of a sample not being representative of the population. This risk exists for judgment and statistical samples.
C. Statistical sampling can use generalized audit software, but it is not required.
D. The tolerable error rate must be predetermined for both judgment and statistical sampling.

A1-52 What is the **BEST** action for an IS auditor to take when an outsourced monitoring process for remote access is inadequate and management disagrees because intrusion detection system (IDS) and firewall controls are in place?

A. Revise the finding in the audit report per management's feedback.
B. Retract the finding because the IDS controls are in place.
C. Retract the finding because the firewall rules are monitored.
D. Document the identified finding in the audit report.

D is the correct answer.

Justification:

A. The IS auditor may include the management response in the report, but that will not affect the requirement to report the finding.
B. The finding remains valid and the management response is documented; however, the audit may indicate a need to review the validity of the management response.
C. The finding remains valid and the management response is documented; however, the audit may indicate a need to review the validity of the management response.
D. IS auditor independence dictates that the additional information provided by the auditee is taken into consideration. Normally, an IS auditor does not automatically retract or revise the finding.

A1-53 An organization uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes and terminations) are completed and delivered to the bank, which prepares the checks and reports for distribution. To **BEST** ensure payroll data accuracy:

A. Payroll reports should be compared to input forms.
B. Gross payroll should be recalculated manually.
C. Checks should be compared to input forms.
D. Checks should be reconciled with output reports.

A is the correct answer.

Justification:

A. The best way to confirm data accuracy, when input is provided by the organization and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports.
B. Recalculating gross payroll manually only verifies whether the processing is correct and not the data accuracy of inputs.
C. Comparing checks to input forms is not feasible because checks contain the processed information and input forms contain the input data.
D. Reconciling checks with output reports only confirms that checks were issued as stated on output reports.

A1-54 Which of the following represents the **GREATEST** potential risk in an electronic data interchange (EDI) environment?

A. Lack of transaction authorizations
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to, or after, establishment of application controls

A is the correct answer.

Justification:

A. **Because the interaction between parties is electronic, there is no inherent authentication occurring; therefore, lack of transaction authorization is the greatest risk.**
B. Loss or duplication of electronic data interchange transmissions is an example of risk, but because all transactions should be logged, the impact is not as great as that of unauthorized transactions.
C. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.
D. Deletion or manipulation of transactions prior to, or after, establishment of application controls is an example of risk. Logging detects any alteration to the data, and the impact is not as great as that of unauthorized transactions.

A1-55 During the planning stage of an IS audit, the **PRIMARY** goal of an IS auditor is to:

A. Address audit objectives.
B. Collect sufficient evidence.
C. Specify appropriate tests.
D. Minimize audit resources.

A is the correct answer.

Justification:

A. **ISACA IS Audit and Assurance Standards require that an IS auditor plan the audit work to address the audit objectives. The activities described in the other options are all undertaken to address audit objectives and, thus, are secondary.**
B. The IS auditor does not collect evidence in the planning stage of an audit.
C. Specifying appropriate tests is not the primary goal of audit planning.
D. Effective use of audit resources is a goal of audit planning, not minimizing audit resources.

A1-56 When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. Sufficient evidence will be collected.
B. Significant deficiencies will be corrected within a reasonable period.
C. All material weaknesses will be identified.
D. Audit costs will be kept at a minimum level.

A is the correct answer.

Justification:

A. **Procedures are processes that an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment that is appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising during an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate, and the IS auditor's past experience plays a key role in making a judgment. The IS auditor should use judgment in assessing the sufficiency of evidence to be collected. ISACA's guidelines provide information on how to meet the standards when performing IS audit work.**
B. The correction of deficiencies is the responsibility of management and is not a part of the audit procedure selection process.
C. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit, and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit. Audit procedures and use of professional judgment cannot ensure that all deficiencies/weaknesses will be identified and corrected.
D. Professional judgment ensures that audit resources and costs are used wisely, but this is not the primary objective of the auditor when selecting audit procedures.

A1-57 A substantive test to verify that tape library inventory records are accurate is:

A. Determining whether bar code readers are installed.
B. Determining whether the movement of tapes is authorized.
C. Conducting a physical count of the tape inventory.
D. Checking whether receipts and issues of tapes are accurately recorded.

C is the correct answer.

Justification:

A. Determining whether bar code readers are installed is a compliance test.
B. Determining whether the movement of tapes is authorized is a compliance test.
C. **A substantive test includes gathering evidence to evaluate the integrity (i.e., the completeness, accuracy and validity) of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test.**
D. Checking whether receipts and issues of tapes are accurately recorded is a compliance test.

A1-58 An appropriate control for ensuring the authenticity of orders received in an electronic data interchange system application is to:

A. Acknowledge receipt of electronic orders with a confirmation message.
B. Perform reasonableness checks on quantities ordered before filling orders.
C. Verify the identity of senders and determine if orders correspond to contract terms.
D. Encrypt electronic orders.

C is the correct answer.

Justification:

A. Acknowledging the receipt of electronic orders with a confirming message is good practice but will not authenticate orders from customers.
B. Performing reasonableness checks on quantities ordered before placing orders is a control for ensuring the correctness of the organization's orders, not the authenticity of its customers' orders.
C. An electronic data interchange system is subject not only to the usual risk exposures of computer systems but also to those arising from the potential ineffectiveness of controls on the part of the trading partner and the third-party service provider, making authentication of users and messages a major security concern.
D. Encrypting sensitive messages is an appropriate step but does not prove authenticity of messages received.

A1-59 An IS auditor finds that the answers received during an interview with a payroll clerk do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequate.
B. expand the scope to include substantive testing.
C. place greater reliance on previous audits.
D. suspend the audit.

B is the correct answer.

Justification:

A. Based solely on the interview with the payroll clerk, the IS auditor will not be able to collect evidence to conclude on the adequacy of existing controls.
B. If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests.
C. Placing greater reliance on previous audits is an inappropriate action, because it provides no current knowledge of the adequacy of the existing controls.
D. Suspending the audit is an inappropriate action, because it provides no current knowledge of the adequacy of the existing controls.

A1-60 An external IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommending a specific vendor product to address this vulnerability. The IS auditor has failed to exercise:

A. Professional independence.
B. Organizational independence.
C. Technical competence.
D. Professional competence.

A is the correct answer.

Justification:

A. **When an IS auditor recommends a specific vendor, the auditor's professional independence is compromised.**
B. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement.
C. Technical competence is not relevant to the requirement of independence.
D. Professional competence is not relevant to the requirement of independence.

A1-61 The **PRIMARY** reason an IS auditor performs a functional walk-through during the preliminary phase of an audit assignment is to:

A. Understand the business process.
B. Comply with auditing standards.
C. Identify control weakness.
D. Develop the risk assessment.

A is the correct answer.

Justification:

A. **Understanding the business process is the first step an IS auditor needs to perform.**
B. ISACA IS Audit and Assurance Standards encourage adoption of the audit procedures/processes required to assist the IS auditor in performing IS audits more effectively. However, standards do not require an IS auditor to perform a process walk-through at the commencement of an audit engagement.
C. Identifying control weaknesses is not the primary reason for the walk-through and typically occurs at a later stage in the audit.
D. The main reason is to understand the business process. The risk assessment is developed after the business process is understood.

A1-62 In the process of evaluating program change controls, an IS auditor uses source code comparison software to:

A. Examine source program changes without information from IS personnel.
B. Detect a source program change made between acquiring a copy of the source and the comparison run.
C. Confirm that the control copy is the current version of the production program.
D. Ensure that all changes made in the current source copy are tested.

A is the correct answer.

Justification:

A. When an IS auditor uses a source code comparison to examine source program changes without information from IS personnel, the IS auditor has an objective, independent and relatively complete assurance of program changes, because the source code comparison identifies the changes.
B. The changes detected by the source code comparison are between two versions of the software. This does not detect changes made since the acquisition of the copy of the software.
C. This is a function of library management, not source code comparison. An IS auditor gains this assurance separately.
D. Source code comparison detects all changes between an original and a changed program; however, the comparison will not ensure that the changes have been adequately tested.

A1-63 The **PRIMARY** purpose for meeting with auditees prior to formally closing a review is to:

A. Confirm that the auditors did not overlook any important issues.
B. Gain agreement on the findings.
C. Receive feedback on the adequacy of the audit procedures.
D. Test the structure of the final presentation.

B is the correct answer.

Justification:

A. The closing meeting identifies any misunderstandings or errors in the audit but does not identify any important issues overlooked in the audit.
B. The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings and responses from management.
C. The closing meeting may obtain comments from management on the conduct of the audit but is not intended to be a formal review of the adequacy of the audit procedures.
D. The structure of an audit report and the presentation follows accepted standards and practices. The closing meeting may indicate errors in the audit or presentation but is not intended to test the structure of the presentation.

A1-64 Which of the following audit techniques **BEST** helps an IS auditor in determining whether there have been unauthorized program changes since the last authorized program update?

A. Test data run
B. Code review
C. Automated code comparison
D. Review of code migration procedures

C is the correct answer.

Justification:

A. Test data runs permit the auditor to verify the processing of preselected transactions but provide no evidence about unauthorized changes or unexercised portions of a program.
B. Code review is the process of reading program source code listings to determine whether the code follows coding standards or contains potential errors or inefficient statements. A code review can be used as a means of code comparison, but it is inefficient and unlikely to detect any changes in the code, especially in a large program.
C. An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure.
D. The review of code migration procedures does not detect unauthorized program changes.

A1-65 When preparing an audit report, the IS auditor should ensure that the results are supported by:

A. Statements from IS management.
B. Work papers of other auditors.
C. An organizational control self-assessment.
D. Sufficient and appropriate audit evidence.

D is the correct answer.

Justification:

A. Statements from IS management may be included in the audit analysis but these statement alone are not considered a sufficient basis for issuing a report.
B. Work papers from other auditors may be used to substantiate and validate a finding but should not be used without the additional evidence of the work papers from the IS auditor who is preparing the report.
C. The results of a control self-assessment may assist the IS auditor in determining risk and compliance but on its own is not enough to support the audit report.
D. ISACA's IS Audit and Assurance Standard on reporting requires that the IS auditor has sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence that is collected during the review even though the IS auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment can supplement the audit findings.

A1-66 While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The **MOST** important concern for an IS auditor is the:

A. Effectiveness of the QA function because it should interact between project management and user management.
B. Efficiency of the QA function because it should interact with the project implementation team.
C. Effectiveness of the project manager because the project manager should interact with the QA function.
D. Efficiency of the project manager because the QA function needs to communicate with the project implementation team.

A is the correct answer.

Justification:

A. To be effective, the quality assurance (QA) function should be independent of project management. If it is not, project management may put pressure on the QA function to approve an inadequate product.
B. The efficiency of the QA function is not impacted by interacting with the project implementation team. The QA team does not release a product for implementation until it meets QA requirements.
C. The project manager responds to the issues raised by the QA team. This does not impact the effectiveness of the project manager.
D. The QA function's interaction with the project implementation team should not impact the efficiency of the project manager.

A1-67 The final decision to include a material finding in an audit report should be made by the:

A. audit committee.
B. auditee's manager.
C. IS auditor.
D. chief executive officer.

C is the correct answer.

Justification:

A. The audit committee should not impair the independence, professionalism and objectivity of the IS auditor by influencing what is included in the audit report.
B. The IS auditor's manager may recommend what should or should not be included in an audit report, but the auditee's manager should not influence the content of the report.
C. The IS auditor should make the final decision about what to include or exclude from the audit report.
D. The chief executive officer must not provide influence over the content of an audit report because that would be a breach of the independence of the audit function.

A1-68 While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. Audit trail of the versioning of the work papers.
B. Approval of the audit phases.
C. Access rights to the work papers.
D. Confidentiality of the work papers.

D is the correct answer.

Justification:
A. Audit trails do not, by themselves, affect the confidentiality, but are part of the reason for requiring encryption.
B. Audit phase approvals do not, by themselves, affect the confidentiality of the work papers, but are part of the reason for requiring encryption.
C. Access to the work papers should be limited by need to know; however, a lack of encryption breaches the confidentiality of the work papers, not the access rights to the papers.
D. Encryption provides confidentiality for the electronic work papers.

A1-69 The **MOST** important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. Comply with regulatory requirements.
B. Provide a basis for drawing reasonable conclusions.
C. Ensure complete audit coverage.
D. Perform the audit according to the defined scope.

B is the correct answer.

Justification:
A. Complying with regulatory requirements is relevant to an audit but is not the most important reason why sufficient and relevant evidence is required.
B. The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them.
C. Ensuring coverage is relevant to conducting an IS audit but is not the most important reason why sufficient and relevant evidence is required. The reason for obtaining evidence is to ensure that the audit conclusions are factual and accurate.
D. The execution of an audit to meet its defined scope is relevant to an audit but is not the reason why sufficient and relevant evidence is required.

A1-70 After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

A. Expand activities to determine whether an investigation is warranted.
B. Report the matter to the audit committee.
C. Report the possibility of fraud to management.
D. Consult with external legal counsel to determine the course of action to be taken.

A is the correct answer.

Justification:

A. An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended.
B. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation.
C. The IS auditor should report the possibility of fraud to top management only after there is sufficient evidence to launch an investigation. This may be affected by whether management may be involved in the fraud.
D. Normally, the IS auditor does not have authority to consult with external legal counsel.

A1-71 An IS auditor notes that failed login attempts to a core financial system are automatically logged and the logs are retained for a year by the organization. This logging is:

A. An effective preventive control.
B. A valid detective control.
C. Not an adequate control.
D. A corrective control.

C is the correct answer.

Justification:

A. Generation of an activity log is not a preventive control because it cannot prevent inappropriate access.
B. Generation of an activity log is not a detective control because it does not help in detecting inappropriate access unless it is reviewed by appropriate personnel.
C. Generation of an activity log is not a control by itself. It is the review of such a log that makes the activity a control (i.e., generation plus review equals control).
D. Generation of an activity log is not a corrective control because it does not correct the effect of inappropriate access.

A1-72 An organization's IS audit charter should specify the:

A. plans for IS audit engagements.
B. objectives and scope of IS audit engagements.
C. detailed training plan for the IS audit staff.
D. role of the IS audit function.

D is the correct answer.

Justification:

A. Planning is the responsibility of audit management.
B. The objectives and scope of each IS audit should be agreed on in an engagement letter. The charter would specify the objectives and scope of the audit function but not of individual engagements.
C. A training plan that is based on the audit plan should be developed by audit management.
D. An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee.

A1-73 Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

A. Attribute sampling
B. Computer-assisted audit techniques
C. Compliance testing
D. Integrated test facility

B is the correct answer.

Justification:

A. Attribute sampling aids in identifying records meeting specific conditions but does not compare one record to another to identify duplicates. To detect duplicate invoice records, the IS auditor should check all items that meet the criteria and not just a sample of the items.
B. Computer-assisted audit techniques (CAATs) enable the IS auditor to review the entire invoice file to look for those items that meet the selection criteria.
C. Compliance testing determines whether controls procedures are adhered to. Using CAATs is the better option because it is most likely more efficient to search for duplicates.
D. An integrated test facility allows the IS auditor to test transactions through the production system but does not compare records to identify duplicates.

A1-74 When developing a risk management program, what is the **FIRST** activity to be performed?

A. Threat assessment
B. Classification of data
C. Inventory of assets
D. Criticality analysis

C is the correct answer.

Justification:

A. The assets need to be identified first. A listing of the threats that can affect the assets is a later step in the process.
B. Data classification is required for defining access controls and in criticality analysis, but the assets (including data) need be identified before doing classification.
C. Identification of the assets to be protected is the first step in the development of a risk management program.
D. Criticality analysis is a later step in the process after the assets have been identified.

A1-75 When evaluating the controls of an electronic data interchange (EDI) application, an IS auditor should **PRIMARILY** be concerned with the risk of:

A. Excessive transaction turnaround time.
B. Application interface failure.
C. Improper transaction authorization.
D. Nonvalidated batch totals.

C is the correct answer.

Justification:

A. An excessive turnaround time is an inconvenience, but not a serious risk.
B. The failure of the application interface is a risk, but not the most serious issue. Usually such a problem is temporary and easily fixed.
C. Foremost among the risk associated with electronic data interchange (EDI) is improper transaction authorization. Because the interaction with the parties is electronic, there is no inherent authentication. Improper authentication poses a serious risk of financial loss.
D. The integrity of EDI transactions is important, but not as significant as the risk of unauthorized transactions

A1-76 Which of the following would be **MOST** useful for an IS auditor for accessing and analyzing digital data to collect relevant audit evidence from diverse software environments?

A. Structured Query Language
B. Application software reports
C. Data analytics controls
D. Computer-assisted auditing techniques

D is the correct answer.

Justification:

A. Structured Query Language provides options for auditors to query specific tables of a database according to audit objectives. However, skills are required to query specific databases, and a user must be able to understand the record structure to access the data.
B. Reports from application software may be useful, but they are not be as beneficial as computer-assisted auditing techniques (CAATs).
C. Data analytics controls might be a good technique to use for control testing, but they are not as comprehensive as CAATs.
D. CAATs are tools used for accessing data in an electronic form from diverse software environments, record formats, etc. CAATs serve as useful tools for collecting and evaluating audit evidence according to audit objectives and can create efficiencies for collecting this evidence.

A1-77 Which of the following sampling methods is the **MOST** appropriate for testing automated invoice authorization controls to ensure that exceptions are not made for specific users?

A. Variable sampling
B. Judgmental sampling
C. Stratified random sampling
D. Systematic sampling

C is the correct answer.

Justification:

A. Variable sampling is used for substantive testing to determine the monetary or volumetric impact of characteristics of a population. This is not the most appropriate in this case.
B. In judgmental sampling, professionals place a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception or all negatives). It should be noted that a judgmental sample is not statistically based, and results should not be extrapolated over the population because the sample is unlikely to be representative of the population.
C. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum. This method of sampling ensures that all sampling units in each subgroup have a known, nonzero chance of selection. It is the most appropriate in this case.
D. Systematic sampling involves selecting sampling units using a fixed interval between selections with the first interval having a random start. This is not the most appropriate in this case.

A1-78 An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

A. decline the assignment.
B. inform management of the possible conflict of interest after completing the audit assignment.
C. inform the BCP team of the possible conflict of interest prior to beginning the assignment.
D. communicate the possibility of conflict of interest to audit management prior to starting the assignment.

D is the correct answer.

Justification:

A. Declining the assignment could be acceptable only after obtaining management approval or it is appropriately disclosed to management, audit management and other stakeholders.
B. Approval should be obtained prior to commencement and not after the completion of the assignment.
C. Informing the BCP team of the possible conflict of interest prior to starting the assignment is not the correct answer because the BCP team does not have the authority to decide on this issue.
D. A possible conflict of interest, likely to affect the IS auditor's independence, should be brought to the attention of management prior to starting the assignment.

A1-79 The **PRIMARY** purpose of an IT forensic audit is:

A. To participate in investigations related to corporate fraud.
B. The systematic collection and analysis of evidence after a system irregularity.
C. To assess the correctness of an organization's financial statements.
D. To preserve evidence of criminal activity.

B is the correct answer.

Justification:
A. Forensic audits are not limited to corporate fraud.
B. The systematic collection and analysis of evidence after a system irregularity best describes a forensic audit. The evidence collected can then be analyzed and used in judicial proceedings.
C. Assessing the correctness of an organization's financial statements is not the primary purpose of most forensic audits.
D. Forensics is the investigation of evidence related to a crime or misbehavior. Preserving evidence is the forensic process, but not the primary purpose.

A1-80 An IS auditor reviews one day of logs for a remotely managed server and finds one case where logging failed, and the backup restarts cannot be confirmed. What should the IS auditor do?

A. Issue an audit finding.
B. Seek an explanation from IS management.
C. Review the classifications of data held on the server.
D. Expand the sample of logs reviewed.

D is the correct answer.

Justification:
A. At this stage it is too preliminary to issue an audit finding. Seeking an explanation from management is advisable, but it is better to gather additional evidence to properly evaluate the seriousness of the situation.
B. Without gathering more information on the incident and the frequency of the incident, it is difficult to obtain a meaningful explanation from management.
C. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.
D. IS Audit and Assurance Standards require that an IS auditor gather sufficient and appropriate audit evidence. The IS auditor has found a potential problem and now needs to determine whether this is an isolated incident or a systematic control failure.

A1-81 In a small organization, the function of release manager and application programmer are performed by the same employee. What is the **BEST** compensating control in this scenario?

A. Hiring additional staff to provide segregation of duties
B. Preventing the release manager from making program modifications
C. Logging of changes to development libraries
D. Verifying that only approved program changes are implemented

D is the correct answer.

Justification:
A. Establishing segregation of duties is not a compensating control; it is a preventive control. In a small organization, it may not be feasible to hire new staff, which is why a compensating control may be necessary.
B. Since the release manager is performing dual roles, preventing them from making program modifications is not feasible, and, in a small organization, segregation of duties may not be possible.
C. Logging changes to development libraries does not detect changes to production libraries.
D. Compensating controls are used to mitigate risk when proper controls are not feasible or practical. In a small organization, it may not be feasible to hire new staff, which is why a compensating control may be necessary. Verifying program changes has roughly the same effect as intended by full segregation of duties.

A1-82 Which of the following is the **FIRST** step in an IT risk assessment for a risk-based audit?

A. Identify all IT systems and controls that are relevant to audit objectives.
B. List all controls from the audit program to select ones matching with audit objectives.
C. Review the results of a risk self-assessment.
D. Understand the business, its operating model and key processes.

D is the correct answer.

Justification:
A. Understanding the business environment comes first; this is followed by understanding the IT environment.
B. Listing controls and matching them to audit objectives is not the first step of risk assessment. This step follows understanding the business environment and the IT systems.
C. A risk self-assessment is optional and applicable for some types of audit engagements.
D. Risk-based auditing must be based on the understanding of the business, operating model and environment. This is the first step in an IT risk assessment for a risk-based audit.

A1-83 An IS auditor discovers that devices connected to the network are not included in a network diagram that had been used to develop the scope of the audit. The chief information officer explains that the diagram is being updated and awaiting final approval. The IS auditor should **FIRST**:

A. expand the scope of the IS audit to include the devices that are not on the network diagram.
B. evaluate the impact of the undocumented devices on the audit scope.
C. note a control deficiency because the network diagram has not been approved.
D. plan follow-up audits of the undocumented devices.

B is the correct answer.

Justification:

A. It is important that the IS auditor does not immediately assume that everything on the network diagram provides information about the risk affecting a network/system. There is a process in place for documenting and updating the network diagram.
B. In a risk-based approach to an IS audit, the scope is determined by the impact that the devices will have on the audit. If the undocumented devices do not impact the audit scope, then they may be excluded from the current audit engagement. The information provided on a network diagram can vary depending on what is being illustrated—for example, the network layer and cross connections.
C. In this case, there is simply a mismatch in timing between the completion of the approval process and when the IS audit began. There is no control deficiency to be reported.
D. Planning for follow-up audits of the undocumented devices is contingent on the risk that the undocumented devices have on the ability of the entity to meet the audit scope.

A1-84 An IS auditor is testing employee access to a large financial system, and the IS auditor selected a sample from the current employee list provided by the auditee. Which of the following evidence is the **MOST** reliable to support the testing?

A. A spreadsheet provided by the system administrator
B. Human resources access documents signed by employees' managers
C. A list of accounts with access levels generated by the system
D. Observations performed onsite in the presence of a system administrator

C is the correct answer.

Justification:

A. A spreadsheet supplied by the system administrator may not be complete or may be inaccurate. Documentary evidence should be collected to support the auditee's spreadsheet.
B. The human resources access documents signed by managers are good evidence; however, they are not as objective as the system-generated access list, because access may have changed, or the documents may have been incorrect when they were signed.
C. The access list generated by the system is the most reliable, because it is the most objective evidence to perform a comparison against the samples selected. The evidence is objective, because it was generated by the system rather than by an individual.
D. The observations are good evidence to understand the internal control structure; however, observations are not efficient for many users. Observations are not objective enough for substantive tests.

A1-85 During a compliance audit of a small bank, the IS auditor notes that the IT and accounting functions are being performed by the same user of the financial system. Which of the following reviews that are conducted by the user's supervisor represents the **BEST** compensating control?

A. Audit trails that show the date and time of the transaction
B. A daily report with the total numbers and dollar amounts of each transaction
C. User account administration
D. Computer log files that show individual transactions

D is the correct answer.

Justification:

A. An audit trail of only the date and time of the transaction is not sufficient to compensate for the risk of multiple functions being performed by the same individual.
B. Review of the summary financial reports does not compensate for the segregation of duties issue.
C. Supervisor review of user account administration can be a good control; however, it may not detect inappropriate activities where a person fills multiple roles.
D. Computer logs record the activities of individuals during their access to a computer system or data file and record any abnormal activities, such as the modification or deletion of financial data.

A1-86 A system developer transfers to the audit department to serve as an IT auditor. When production systems are to be reviewed by this employee, which of the following will become the **MOST** significant concern?

A. The work may be construed as a self-audit.
B. Audit points may largely shift to technical aspects.
C. The employee may not have sufficient control assessment skills.
D. The employee's knowledge of business risk may be limited.

A is the correct answer.

Justification:

A. Because the employee had been a developer, it is recommended that the audit coverage should exclude the systems developed by this employee to avoid any conflicts of interests.
B. Because the employee has a technical background, it is possible that the audit findings tend to focus on technical matters. However, this is normally corrected in the review process before it is carried out in production.
C. Because auditing is a new role for this employee, they may not have adequate control assessment skills. However, this can be addressed by on-the-job training and is not be as big of a concern as a potential conflict of interest.
D. Because this employee was previously employed in the organization's IT department, it is possible to build upon the employee's current understanding of the business to address any gaps in knowledge.

A1-87 Which of the following **BEST** describes the objective of an IS auditor discussing the audit findings with the auditee?

A. Communicate results to the auditee.
B. Develop time lines for the implementation of suggested recommendations.
C. Confirm the findings and propose a course of corrective action.
D. Identify compensating controls to the identified risk.

C is the correct answer.

Justification:

A. Based on this discussion, the IS auditor will finalize the report and present the report to relevant levels of senior management after the findings are confirmed. This discussion should, however, also address a timetable for remediation of the audit findings.
B. This discussion informs management of the findings of the audit, and, based on these discussions, management may agree to develop an implementation plan for the suggested recommendations, along with the time lines.
C. Before communicating the results of an audit to senior management, the IS auditor should discuss the findings with the auditee. The goal of this discussion is to confirm the accuracy of the findings and to propose or recommend a course of corrective action.
D. At the draft report stage, the IS auditor may recommend various controls to mitigate the risk, but the purpose of the meeting is to validate the findings of the audit with management.

A1-88 Which of the following responsibilities would **MOST** likely compromise the independence of an IS auditor when reviewing the risk management process?

A. Participating in the design of the risk management framework
B. Advising on different implementation techniques
C. Facilitating risk awareness training
D. Performing a due diligence review of the risk management processes

A is the correct answer.

Justification:

A. Participating in the design of the risk management framework involves designing controls, which compromises the independence of the IS auditor to audit the risk management process.
B. Advising on different implementation techniques does not compromise the IS auditor's independence because the IS auditor will not be involved in the decision-making process.
C. Facilitating awareness training does not hamper the IS auditor's independence because the auditor will not be involved in the decision-making process.
D. Due diligence reviews are a type of audit generally related to mergers and acquisitions.

A1-89 Which of the following would be the **GREATEST** concern if audit objectives are not established during the initial phase of an audit program?

A. Key stakeholders are incorrectly identified.
B. Control costs will exceed planned budget.
C. Important business risk may be overlooked.
D. Previously audited areas may be inadvertently included.

C is the correct answer.

Justification:
A. In certain cases, it may be more difficult to discuss findings when incorrect stakeholders are identified, thus delaying the communication of audit findings. However, this is not as concerning as important business risk not being included in audit scope.
B. Many factors determine the cost of controls. Therefore, it is difficult to state that only audit objectives will determine the control cost. However, this is not as important if key risk is not identified.
C. **Without an audit scope, the appropriate risk assessment has not been performed, and therefore, the auditor might not audit those areas of highest risk for the organization.**
D. Auditing previously audited areas is not an efficient use of resources; however, this is not as big of a concern as key risk not being identified.

A1-90 An IS auditor wants to analyze audit trails on critical servers to discover potential anomalies in user or system behavior. Which of the following is the **MOST** suitable for performing that task?

A. Computer-aided software engineering tools
B. Embedded data collection tools
C. Trend/variance detection tools
D. Heuristic scanning tools

C is the correct answer.

Justification:
A. Computer-aided software engineering tools are used to assist in software development.
B. Embedded (audit) data collection software, such as systems control audit review file or systems audit review file, is used to provide sampling and production statistics, but not to conduct an audit log analysis.
C. **Trend/variance detection tools look for anomalies in user or system behavior, such as invoices with increasing invoice numbers.**
D. Heuristic scanning tools are a type of virus scanning used to indicate possible infected traffic.

A1-91 While performing an audit of an accounting application's internal data integrity controls, an IS auditor identifies a major control deficiency in the change management software supporting the accounting application. The **MOST** appropriate action for the IS auditor to take is to:

A. Continue to test the accounting application controls and inform the IT manager about the control deficiency and recommend possible solutions.
B. Complete the audit and not report the control deficiency because it is not part of the audit scope.
C. Continue to test the accounting application controls and include the deficiency in the final report.
D. Cease all audit activity until the control deficiency is resolved.

C is the correct answer.

Justification:

A. The IS auditor should not assume that the IT manager will follow through on a verbal notification to resolve the change management control deficiency, and it is inappropriate to offer consulting services on issues discovered during an audit.
B. Although not technically within the audit scope, it is the responsibility of the IS auditor to report findings discovered during an audit that can have a material impact on the effectiveness of controls.
C. It is the responsibility of the IS auditor to report on findings that can have a material impact on the effectiveness of controls—whether or not they are within the scope of the audit.
D. It is not the role of the IS auditor to demand that IT work be completed before performing or completing an audit.

A1-92 Which of the following will **MOST** successfully identify overlapping key controls in business application systems?

A. Reviewing system functionalities that are attached to complex business processes
B. Submitting test transactions through an integrated test facility
C. Replacing manual monitoring with an automated auditing solution
D. Testing controls to validate that they are effective

C is the correct answer.

Justification:

A. In general, highly complex business processes may have more key controls than business areas with less complexity; however, finding, with certainty, unnecessary controls in complex areas is not always possible. If a well-thought-out key control structure was established from the beginning, finding any overlap in key controls will not be possible.
B. An integrated test facility is an audit technique to test the accuracy of the processes in the application system. It may find control flaws in the application system, but it would be difficult to find the overlap in key controls.
C. As part of the effort to realize continuous audit management, there are cases for introducing an automated monitoring and auditing solution. All key controls need to be clearly aligned for systematic implementation; thus, analysts can discover unnecessary or overlapping key controls in existing systems.
D. By testing controls to validate whether they are effective, the IS auditor can identify whether there are overlapping controls; however, the process of implementing an automated auditing solution would better identify overlapping controls.

A1-93 When performing a risk analysis, the IS auditor should **FIRST**:

A. Review the data classification program.
B. Identify the organization's information assets.
C. Identify the inherent risk of the system.
D. Perform a cost-benefit analysis for controls.

B is the correct answer.

Justification:

A. After the business objectives and the underlying systems are identified, the greatest degree of risk management effort should be focused towards those assets containing data considered most sensitive to the organization. The data classification program assists the IS auditor in identifying these assets.
B. The first step of the risk assessment process is to identify the systems and processes that support the business objectives because risk to those processes impacts the achievement of business goals.
C. Inherent risk is the exposure without considering the actions that management has taken or might take. The purpose of a risk assessment is to identify vulnerabilities so that mitigating controls can be established. However, one must first understand the business and its supporting systems to best identify systems requiring the most risk assessment effort.
D. Designing and implementing controls to mitigate inherent risk of critical systems can only be performed after the above steps have been taken.

A1-94 After identifying the findings, the IS auditor should **FIRST**:

A. Gain agreement on the findings.
B. Determine mitigation measures for the findings.
C. Inform senior management of the findings.
D. Obtain remediation deadlines to close the findings.

A is the correct answer.

Justification:

A. If findings are not agreed upon and confirmed by both parties, then there may be an issue during sign-off on the final audit report or while discussing findings with management. When agreement is obtained with the auditee, it implies the finding is understood and a clear plan of action can be determined.
B. Although the auditor may recommend mitigation measures, the organization ultimately decides and implements the mitigation strategies as a function of risk management.
C. Before senior management is informed, it is imperative that the auditor informs the auditee and gains agreement on the audit findings to correctly communicate the risk.
D. Obtaining remediation deadlines to close the findings is not the first step in communicating the audit findings.

A1-95 A **PRIMARY** benefit derived for an organization employing control self-assessment techniques is that it:

A. Can identify high-risk areas that might need a detailed review later.
B. Allows IS auditors to independently assess risk.
C. Can be used as a replacement for traditional audits.
D. Allows management to relinquish responsibility for control.

A is the correct answer.

Justification:

A. **Control self-assessment (CSA) is predicated on the review of high-risk areas that either need immediate attention or may require a more thorough review later.**
B. CSA requires the involvement of IS auditors and line management. The internal audit function shifts some of the control monitoring responsibilities to the functional areas.
C. CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them.
D. CSA does not allow management to relinquish its responsibility for control.

A1-96 Which of the following is the **FIRST** step performed prior to creating a risk ranking for the annual internal IS audit plan?

A. Prioritize the identified risk.
B. Define the audit universe.
C. Identify the critical controls.
D. Determine the testing approach.

B is the correct answer.

Justification:

A. After the audit universe is defined, the IS auditor can prioritize risk based on its overall impact on different operational areas of the organization covered under the audit universe.
B. **In a risk-based audit approach, the IS auditor identifies risk to the organization based on the nature of the business. To plan an annual audit cycle, the types of risk must be ranked. To rank the types of risk, the auditor must first define the audit universe by considering the IT strategic plan, organizational structure and authorization matrix.**
C. The controls that help in mitigating high-risk areas are generally critical controls and their effectiveness provides assurance on mitigation of risk. However, this cannot be done unless the types of risk are ranked.
D. The testing approach is based on the risk ranking.

A1-97 Which of the following is **MOST** likely be considered a conflict of interest for an IS auditor who is reviewing a cybersecurity implementation?

A. Delivering cybersecurity awareness training
B. Designing the cybersecurity controls
C. Advising on the cybersecurity framework
D. Conducting the vulnerability assessment

B is the correct answer.

Justification:
A. Delivering cybersecurity awareness training is typically an operational responsibility, but it is not nearly as strong as a conflict of interest as the auditor designing controls and then reviewing them.
B. If an auditor designs the controls, a conflict of interest arises in the neutrality of the auditor to address deficiencies during an audit. This is in violation of the ISACA Code of Ethics.
C. Part of the role of an IS auditor can be to advise on a cybersecurity framework, provided that such advice does not rise to the level of designing specific controls that the auditor would later review.
D. Conducting a vulnerability assessment can be the responsibility of the IS auditor and does not present a conflict of interest.

A1-98 An IS auditor identified a business process to be audited. The IS auditor should **NEXT** identify the:

A. Most valuable information assets.
B. IS audit resources to be deployed.
C. Auditee personnel to be interviewed.
D. Control objectives and activities.

D is the correct answer.

Justification:
A. All assets need to be identified, not just information assets. To determine the key information assets to be audited, the IS auditor should first determine which control objectives and key control activities should be validated. Only information assets that are related to the control objectives and key control activities are relevant for scoping the audit.
B. Only after determining which controls and related relevant information assets are to be validated can the IS auditor decide on the key IS audit resources (with the relevant skill sets) that should be deployed for the audit.
C. Only after determining the key control activities to be validated can the IS auditor identify the relevant process personnel who should be interviewed.
D. After the business process is identified, the IS auditor should first identify the control objectives and activities associated with the business process that should be validated in the audit.

A1-99 The effect of which of the following should have priority in planning the scope and objectives of an IS audit?

A. Applicable statutory requirements
B. Applicable corporate standards
C. Applicable industry good practices
D. Organizational policies and procedures

A is the correct answer.

Justification:

A. **The effect of applicable statutory requirements must be factored in while planning an IS audit—the IS auditor has no options regarding statutory requirements because there can be no limitation of scope relating to statutory requirements.**
B. Statutory requirements always take priority over corporate standards.
C. Industry good practices help plan an audit; however, good practices are not mandatory and can be deviated from, to meet organization objectives.
D. Organizational policies and procedures are important, but statutory requirements always take priority. Organizational policies must be in alignment with statutory requirements.

A1-100 An external IS auditor discovers that systems in the scope of the audit were implemented by an associate. In such a circumstance, IS audit management should:

A. Remove the IS auditor from the engagement.
B. Cancel the engagement.
C. Disclose the issue to the client.
D. Take steps to restore the IS auditor's independence.

C is the correct answer.

Justification:

A. It is not necessary to withdraw the IS auditor unless there is a statutory limitation, which exists in certain countries.
B. Canceling the engagement is not required if properly disclosed and accepted.
C. **In circumstances in which the IS auditor's independence is impaired and the IS auditor continues to be associated with the audit, the facts surrounding the issue of the IS auditor's independence should be disclosed to the appropriate management and in the report.**
D. This is not a feasible solution. The independence of the IS auditor cannot be restored while continuing to conduct the audit.

A1-101 An IS auditor is planning to evaluate the control design effectiveness that is related to an automated billing process. Which of the following is the **MOST** effective approach for the auditor to adopt?

A. Interview
B. Inquiry
C. Reperformance
D. Walk-through

D is the correct answer.

Justification:

A. An interview is not as strong an evidence as an observation or walk-throughs. In addition, personnel might add some bias to interviews if they know they are being interviewed for an audit.
B. Inquiry can be used to understand the controls in a process only if it is accompanied by verification of evidence. However, interviewees might be biased if they know they are being audited.
C. Reperformance is used to evaluate the operating effectiveness of the control rather than the design of the control.
D. Walk-throughs involve a combination of inquiry and inspection of evidence with respect to business process controls. This is the most effective basis for evaluation of the design of the control, because it actually exists.

A1-102 Which of the following is the **MAIN** reason to perform a risk assessment in the planning phase of an IS audit?

A. To ensure management's concerns are addressed
B. To provide reasonable assurance material items will be addressed
C. To ensure the audit team will perform audits within budget
D. To develop audit program and procedures needed to perform the audit

B is the correct answer.

Justification:

A. Management concerns have no bearing on the risk assessment process. If management has concerns and wants the auditor to focus on a certain area, the auditor should ensure adequate time is allocated to address the concerns.
B. A risk assessment helps to focus the audit procedures on the highest risk areas included in the scope of the audit. The concept of reasonable assurance is also important.
C. A risk assessment is performed to determine where to place time and personnel resources, while budget constraints are limited to time resources.
D. A risk assessment is not used in the development of the audit program and procedures. However, the risk assessment is used to allocate resources to audits.

A1-103 Which of the following is **MOST** important to ensure before communicating the audit findings to top management during the closing meeting?

A. Risk statement includes an explanation of a business impact.
B. Findings are clearly tracked back to evidence.
C. Recommendations address root causes of findings.
D. Remediation plans are provided by responsible parties.

B is the correct answer.

Justification:
A. It is important to have a well-elaborated risk statement; however, it might not be relevant if findings are not accurate.
B. Without adequate evidence, the findings hold no ground; therefore, this must be verified before communicating the findings.
C. It is important to address the root causes of findings, and it may be not included in the report. However, it might not be relevant if findings are not accurate.
D. In some cases, top-management might expect to see remediation plans during debriefing of the findings; however, the accuracy of findings should be proved first.

A1-104 The **MAIN** advantage of an IS auditor directly extracting data from a general ledger systems is:

A. Reduction of human resources needed to support the audit
B. Reduction in the time to have access to the information
C. Greater flexibility for the audit department
D. Greater assurance of data validity

D is the correct answer.

Justification:
A. Although the burden on human resources to support the audit may decrease if the IS auditor directly extracts the dates, this advantage is not as significant as the increased data validity.
B. This will not necessarily reduce the time to have access to the information because time will need to be scheduled for training and granting access.
C. There may be more flexibility for the IS auditor to adjust the data extracts to meet various audit requirements; however, this is not the main advantage.
D. If the IS auditor executes the data extraction, there is greater assurance that the extraction criteria will not interfere with the required completeness, and, therefore, all required data will be collected. Asking IT to extract the data may expose the risk of filtering out exceptions that should be seen by the auditor. Also, if the IS auditor collects the data, all internal references correlating the various data tables/elements will be understood, and this knowledge may reveal vital elements to the completeness and correctness of the overall audit activity.

A1-105 An IS auditor wants to determine the number of purchase orders that are not appropriately approved. Which of the following sampling techniques should an IS auditor use to make such a conclusion?

A. Attribute
B. Variable
C. Stop-or-go
D. Judgment

A is the correct answer.

Justification:

A. Attribute sampling is used to test compliance of transactions to controls—in this instance, the existence of appropriate approval.
B. Variable sampling is used in substantive testing situations and deals with population characteristics that vary, such as monetary values and weights.
C. Stop-or-go sampling is used when the expected occurrence rate is extremely low.
D. Judgment sampling is not relevant here. It refers to a subjective approach of determining sample size and selection criteria of elements of the sample.

A1-106 An IS auditor uses computer-assisted audit techniques (CAATs) to collect and analyze data. Which of the following attributes of evidence is **MOST** affected by using CAATs?

A. Usefulness
B. Reliability
C. Relevance
D. Adequacy

B is the correct answer.

Justification:

A. Usefulness of audit evidence pulled by computer-assisted audit techniques (CAATs) is determined by the audit objective, and the use of CAATs does not have as direct of an impact on usefulness as reliability.
B. Because the data are directly collected by the IS auditor, the audit findings can be reported with an emphasis on the reliability of the records that are produced and maintained in the system. The reliability of the source of information used provides reassurance on the generated findings.
C. Relevance of audit evidence pulled by CAATs is determined by the audit objective, and the use of CAATs does not have as direct of an impact on relevance as reliability.
D. Adequacy of audit evidence pulled by CAATs is determined by the processes and personnel who author the data, and the use of CAATs does not have any impact on competence.

A1-107 An internal IS audit function is planning a general IS audit. Which of the following activities takes place during the **FIRST** step of the planning phase?

A. Development of an audit program
B. Define the audit scope
C. Identification of key information owners
D. Development of a risk assessment

D is the correct answer.

Justification:
A. The results of the risk assessment are used for the input for the audit program.
B. The output of the risk assessment helps define the scope.
C. A risk assessment must be performed prior to identifying key information owners. Key information owners are generally not directly involved during the planning process of an audit.
D. A risk assessment should be performed to determine how internal audit resources should be allocated to ensure that all material items will be addressed.

A1-108 Which of the following is the **MOST** important skill that an IS auditor should develop to understand the constraints of conducting an audit?

A. Managing audit staff
B. Allocating resources
C. Project management
D. Attention to detail

C is the correct answer.

Justification:
A. Managing audit staff is not the only aspect of conducting an audit.
B. Allocating resources, such as time and personnel, are needed for overall project management skills.
C. Audits often involve resource management, deliverables, scheduling and deadlines that are similar to project management good practices.
D. Attention to detail is needed, but it is not a constraint of conducting audits.

A1-109 What is the **MAJOR** benefit of conducting a control self-assessment over a traditional audit?

A. It detects risk sooner.
B. It replaces the internal audit function.
C. It reduces the audit workload.
D. It reduces audit resource requirements.

A is the correct answer.

Justification:
A. Control self-assessments (CSAs) require employees to assess the control stature of their own function. CSAs help to increase the understanding of business risk and internal controls. Because they are conducted more frequently than audits, CSAs help to identify risk in a timelier manner.
B. CSAs do not replace the internal audit function; an audit must still be performed to ensure that controls are present.
C. CSAs may not reduce the audit function's workload and are not a major difference between the two approaches.
D. CSAs do not affect the need for audit resources. Although the results of the CSA may serve as a reference point for the audit process, they do not affect the scope or depth of audit work that needs to be performed.

A1-110 An IS auditor is reviewing a project risk assessment and notices that the overall residual risk level is high due to confidentiality requirements. Which of the following types of risk is normally high due to the number of unauthorized users the project may affect?

A. Control risk
B. Compliance risk
C. Inherent risk
D. Residual risk

C is the correct answer.

Justification:

A. Control risk can be high, but it is not due to internal controls not being identified, evaluated or tested, and is not due to the number of users or business areas affected.
B. Compliance risk is the penalty applied to current and future earnings for nonconformance to laws and regulations and may not be impacted by the number of users and business areas affected.
C. **Inherent risk is normally high due to the number of users and business areas that may be affected. Inherent risk is the risk level or exposure without considering the actions that management has taken or might take.**
D. Residual risk is the remaining risk after management has implemented a risk response and is not based on the number of users or business areas affected.

A1-111 An IS auditor discovers a potential material finding. The **BEST** course of action is to:

A. report the potential finding to business management.
B. discuss the potential finding with the audit committee.
C. increase the scope of the audit.
D. perform additional testing.

D is the correct answer.

Justification:

A. The item should be confirmed through additional testing before it is reported to management.
B. The item should be confirmed through additional testing before it is discussed with the audit committee.
C. Additional testing to confirm the potential finding should be within the scope of the engagement. Increasing the scope could demand more needed audit resources and could be subject to risk creep.
D. **The IS auditor should perform additional testing to ensure that it is a finding. An auditor can quickly lose credibility if it is later discovered the finding was not justified or accurate.**

A1-112 Which of the following is in the **BEST** position to approve changes to the audit charter?

A. Board of directors
B. Audit committee
C. Executive management
D. Director of internal audit

B is the correct answer.

Justification:

A. The board of directors does not need to approve the charter; it is best presented to the audit committee for approval.
B. The audit committee is a subgroup of the board of directors. The audit department should report to the audit committee and the audit charter should be approved by the committee.
C. Executive management is not required to approve the audit charter and will not have the independence to approve the charter. The audit committee is in the best position to approve the charter because it is an independent and senior group.
D. While the director of internal audit may draft the charter and make changes, the audit committee should have the final approval of the charter.

A1-113 An IS auditor reviewing the process of log monitoring wants to evaluate the organization's manual review process. Which of the following audit techniques would the auditor **MOST** likely employ to fulfill this purpose?

A. Inspection
B. Inquiry
C. Walk-through
D. Reperformance

C is the correct answer.

Justification:

A. Inspection is just one component of a walk-through and by itself does not supply enough information to provide a full understanding of the overall process and identify potential control weaknesses.
B. Inquiry provides only general information on how the control is executed. It does not necessarily enable the IS auditor to determine whether the control performer has an in-depth understanding of the control.
C. Walk-through procedures usually include a combination of inquiry, observation, inspection of relevant documentation and reperformance of controls. A walk-through of the manual log review process follows the manual log review process from start to finish to gain a thorough understanding of the overall process and identify potential control weaknesses.
D. Reperformance of the control is carried out by the IS auditor and does not provide assurance of the competency of the auditee.

A1-114 An IS auditor is comparing equipment in production with inventory records. This type of testing is an example of:

A. substantive testing.
B. compliance testing.
C. analytical testing.
D. control testing.

A is the correct answer.

Justification:

A. **Substantive testing obtains audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.**
B. Compliance testing is evidence gathering for the purpose of testing an enterprise's compliance with control procedures. This differs from substantive testing in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.
C. Analytical testing evaluates the relationship of two sets of data and discerns inconsistencies in the relationship.
D. Control testing is the same as compliance testing.

A1-115 Which of the following does a lack of adequate controls represent?

A. An impact
B. A vulnerability
C. An asset
D. A threat

B is the correct answer.

Justification:

A. Impact is the measure of the consequence (including financial loss, reputational damage, loss of customer confidence) that a threat event may have.
B. **The lack of adequate controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers, employee error, environmental threat or equipment failure. This could result in a loss of sensitive information, financial loss, legal penalties or other losses.**
C. An asset is something of either tangible or intangible value worth protecting, including people, systems, infrastructure, finances and reputation.
D. A threat is a potential cause of an unwanted incident.

A1-116 An IS auditor notes daily reconciliation of visitor access card inventory is not aligned with the organization's procedures. Which of the following is the auditor's **BEST** course of action?

A. Do not report the lack of reconciliation.
B. Recommend regular physical inventory counts.
C. Report the lack of daily reconciliations.
D. Recommend the implementation of a more secure access system.

C is the correct answer.

Justification:

A. Absence of discrepancy in physical count only confirms absence of any impact but cannot be a reason to overlook failure of operation of the control. The issue should be reported because the control was not followed.
B. While the IS auditor may in some cases recommend a change in procedures, the primary goal is to observe and report when the current process is deficient.
C. **The IS auditor should report the lack of daily reconciliation as an exception, because a physical inventory count gives assurance only at a point in time and the practice is not in compliance with management's mandated activity.**
D. While the IS auditor may in some cases recommend a more secure solution, the primary goal is to observe and report when the current process is deficient.

A1-117 During an audit, the IS auditor notes the application developer also performs quality assurance testing on another application. Which of the following is the **MOST** important course of action for the auditor?

A. Recommend compensating controls.
B. Review the code created by the developer.
C. Analyze the quality assurance dashboards.
D. Report the identified condition.

D is the correct answer.

Justification:

A. Although compensating controls may be a good idea, the primary response in this case should be to report the condition, because the risk associated with this should be reported to the users of the audit report
B. Evaluating the code created by the application developer is not the appropriate response in this case. The IS auditor may evaluate a sample of changes to determine whether the developer tested his/her own code, but the primary response should be to report the condition.
C. Analyzing the quality assurance dashboards can help evaluate the actual impact of the lack of segregation of duties but does not address the underlying risk. The primary response should be to report the condition.
D. **The software quality assurance role should be independent and separate from development and development activities. The same person should not hold both roles because this would cause a segregation of duties concern. The IS auditor should report this condition when identified.**

A1-118 An IS auditor is reviewing risk and controls of a bank's wire transfer system. To ensure that the bank's financial risk is properly addressed, the IS auditor will most likely review which of the following?

A. Privileged access to the wire transfer system
B. Wire transfer procedures
C. Fraud monitoring controls
D. Employee background checks

B is the correct answer.

Justification:

A. Privileged access, such as administrator access, is necessary to manage user account privileges and should not be granted to end users. The wire transfer procedures are a better control to review to ensure that there is segregation of duties of the end users to help prevent fraud.
B. Wire transfer procedures include segregation of duties controls. This helps prevent internal fraud by not allowing one person to initiate, approve and send a wire. Therefore, the IS auditor should review the procedures as they relate to the wire system.
C. Fraud monitoring is a detective control and does not prevent financial loss. Segregation of duties is a preventive control which is part of the wire transfer procedures.
D. Although controls related to background checks are important, the controls related to segregation of duties as found in the wire transfer procedures are more critical.

A1-119 An IS auditor is determining the appropriate sample size for testing the existence of program change approvals. Previous audits did not indicate any exceptions, and management has confirmed that no exceptions have been reported for the review period. In this context, the IS auditor can adopt a:

A. lower confidence coefficient, resulting in a smaller sample size.
B. higher confidence coefficient, resulting in a smaller sample size.
C. higher confidence coefficient, resulting in a larger sample size.
D. lower confidence coefficient, resulting in a larger sample size.

A is the correct answer.

Justification:

A. When internal controls are strong, a lower confidence coefficient can be adopted, which will enable the use of a smaller sample size.
B. A higher confidence coefficient will result in the use of a larger sample size.
C. A higher confidence coefficient need not be adopted in this situation because internal controls are strong.
D. A lower confidence coefficient will result in the use of a smaller sample size.

A1-120 Why does an audit manager review the staff's audit papers, even when the IS auditors have many years of experience?

A. Internal quality requirements
B. The audit guidelines
C. The audit methodology
D. Professional standards

D is the correct answer.

Justification:

A. Internal quality requirements may exist but are superseded by the requirement of supervision to comply with professional standards.
B. Audit guidelines exist to provide guidance on how to achieve compliance with professional standards. For example, they may provide insights on the purpose of supervision and examples of how supervisory duties are to be performed to achieve compliance with professional standards.
C. An audit methodology is a well-configured process/procedure to achieve audit objectives. While an audit methodology is a meaningful tool, supervision is generally driven by compliance with professional standards.
D. Professional standards from ISACA, The Institute of Internal Auditors and the International Federation of Accountants require supervision of audit staff to accomplish audit objectives and comply with competence, professional proficiency and documentation requirements, and more.

A1-121 Which technique will **BEST** test for the existence of dual control when auditing the wire transfer systems of a bank?

A. Analysis of transaction logs
B. Reperformance
C. Observation
D. Interviewing personnel

C is the correct answer.

Justification:

A. Analysis of transaction logs would help to show that dual control is in place but does not necessarily guarantee that this process is being followed consistently. Therefore, observation is the better test technique.
B. Although reperformance could provide assurance that dual control was in effect, reperforming wire transfers at a bank would not be an option for an IS auditor.
C. Dual control requires that two people carry out an operation. The observation technique helps to ascertain whether two individuals do get involved in execution of the operation and an element of oversight exists. It is obvious if one individual is masquerading and filling in the role of the second person.
D. Interviewing personnel is useful to determine the level of awareness and understanding of the personnel carrying out the operations. However, it does provide direct evidence confirming the existence of dual control, because the information provided may not accurately reflect the process being performed.

A1-122 In a risk-based IS audit, where both inherent and control risk have been assessed as high, an IS auditor would **MOST** likely compensate for this scenario by performing additional:

A. Stop-or-go sampling.
B. Substantive testing.
C. Compliance testing.
D. Discovery sampling.

B is the correct answer.

Justification:
A. Stop-or-go sampling is used when an IS auditor believes few errors will be found in the population, and, thus, is not the best type of testing to perform in this case.
B. Because both the inherent and control risk are high in this case, additional testing is required. Substantive testing obtains audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.
C. Compliance testing is evidence gathering for the purpose of testing an enterprise's compliance with control procedures. Although performing compliance testing is important, performing additional substantive testing is more appropriate in this case.
D. Discovery sampling is a form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population, typically used to test for fraud or other irregularities. In this case, additional substantive testing is the better option.

A1-123 The **PRIMARY** objective of the audit initiation meeting with an IS audit client is to:

A. Discuss the scope of the audit.
B. Identify resource requirements of the audit.
C. Select the methodology of the audit.
D. Collect audit evidence.

A is the correct answer.

Justification:
A. The primary objective of the initiation meeting with an audit client is to help define the scope of the audit.
B. Determining the resource requirements of the IS audit is typically done by IS audit management during the early planning phase of the project rather than at the initiation meeting.
C. Selecting the methodology of the audit is not normally an objective of the initiation meeting.
D. For most audits, collecting audit evidence is performed during the course of the engagement and is not normally collected during the initiation meeting.

A1-124 The **PRIMARY** purpose of the IS audit charter is to:

A. Establish the organizational structure of the audit department.
B. Illustrate the reporting responsibilities of the is audit function.
C. Detail the resource requirements needed for the audit function.
D. Outline the responsibility and authority of the is audit function.

D is the correct answer.

Justification:

A. The IS audit charter does not set forth the organizational structure of the IS audit department. The charter serves as a directive to create the IS audit function.
B. The IS audit charter does not dictate the reporting requirements of the IS audit department. The charter sets forth the purpose, responsibility, authority and accountability of the information systems audit function.
C. Resources are determined by the audit and not the charter.
D. The primary purpose of the IS audit charter is to set forth the purpose, responsibility, authority and accountability of the IS audit function. The charter document grants authority to the audit function on behalf of the board of directors and organization stakeholders.

A1-125 Which of the following is **MOST** important for an IS auditor to understand when auditing an ecommerce environment?

A. The technology architecture of the ecommerce environment
B. The policies, procedures and practices forming the control environment
C. The nature and criticality of the business processes supported by the application
D. Continuous monitoring of control measures for system availability and reliability

C is the correct answer.

Justification:

A. Understanding the technology architecture of the ecommerce environment is important; however, it is vital that the nature and criticality of the business process supported by the ecommerce application are well understood.
B. Although the policies, procedure and practices that form the internal control environment need to be in alignment with the ecommerce environment, this is not the most important element that the IS auditor needs to understand.
C. The ecommerce application enables the execution of business transactions. Therefore, it is important to understand the nature and criticality of the business process supported by the ecommerce application to identify specific controls to review.
D. The availability of the ecommerce environment is important, but this is only one of the aspects to be considered with respect to business processes that are supported by the ecommerce application.

A1-126 During an IS audit, which is the **BEST** method for an IS auditor to evaluate the implementation of segregation of duties within an IT department?

A. Discuss with the IT managers.
B. Review the IT job descriptions.
C. Research past IT audit reports.
D. Evaluate the organizational structure.

A is the correct answer.

Justification:

A. **Discussing the implementation of segregation of duties with the IT managers is the best way to determine how responsibilities are assigned within the department.**
B. Job descriptions may not be the best source of information because they can be outdated or what is documented in the job descriptions may be different from what is actually performed.
C. Past IS audit reports are not the best source of information because they may not accurately describe how IT responsibilities are assigned.
D. Evaluating the organizational structure may give a limited view on the allocation of IT responsibilities. The responsibilities also may have changed over time.

A1-127 A financial institution with multiple branch offices has an automated control that requires the branch manager to approve transactions more than a certain amount. What type of audit control is this?

A. Detective
B. Preventive
C. Corrective
D. Directive

B is the correct answer.

Justification:

A. Detective controls identify events after they have happened. In this case, the action of the branch manager would prevent an event from occurring.
B. **Having a manager approve transactions more than a certain amount is considered a preventive control.**
C. A corrective control serves to remedy problems discovered by detective controls. In this case, the action of the branch manager is a preventive control.
D. A directive control is a manual control that typically consists of a policy or procedure that specifies what actions are to be performed. In this case, there is an automated control that prevents an event from occurring.

A1-128 During an application software review, an IS auditor identified minor weaknesses in a relevant database environment that is out of scope for the audit. The **BEST** option is to:

A. Include a review of the database controls in the scope.
B. Document for future review.
C. Work with database administrators to correct the issue.
D. Report the weaknesses as observed.

D is the correct answer.

Justification:
A. Executing audits and reviews outside the scope is not advisable. In this case, the weakness identified is considered to be a minor issue, and it is sufficient to report the issue and address it at a later time.
B. In this case, the weakness identified is considered to be a minor issue. The IS auditor should formally report the weaknesses as an observation rather than documenting it to address during a future audit.
C. It is not appropriate for the IS auditor to work with database administrators to correct the issue.
D. Any weakness noticed should be reported, even if it is outside the scope of the current audit. Weaknesses identified during an application software review need to be reported to management.

A1-129 A centralized antivirus system determines whether each personal computer has the latest signature files and installs the latest signature files before allowing a PC to connect to the network. This is an example of a:

A. directive control.
B. corrective control.
C. compensating control.
D. detective control.

B is the correct answer.

Justification:
A. Directive controls, such as IT policies and procedures, do not apply in this case because this is an automated control.
B. Corrective controls are designed to correct errors, omissions and unauthorized uses and intrusions, when they are detected. This provides a mechanism to detect when malicious events have happened and correct the situation.
C. A compensating control is used where other controls are not sufficient to protect the system. In this case, the corrective control in place will effectively protect the system from access via an unpatched device.
D. Detective controls exist to detect and report when errors, omissions and unauthorized uses or entries occur.

A1-130 Due to unexpected resource constraints of the IS audit team, the audit plan, as originally approved, cannot be completed. Assuming the situation is communicated in the audit report, which course of action is **MOST** acceptable?

A. Test the adequacy of the control design.
B. Test the operational effectiveness of controls.
C. Focus on auditing high-risk areas.
D. Rely on management testing of controls.

C is the correct answer.

Justification:
A. Testing the adequacy of control design is not the best course of action because this does not ensure that controls operate effectively as designed.
B. Testing control operating effectiveness does not ensure that the audit plan is focused on areas of greatest risk.
C. Reducing the scope and focusing on auditing high-risk areas is the best course of action.
D. The reliance on management testing of controls does not provide an objective verification of the control environment.

A1-131 Which of the following **BEST** ensures the effectiveness of controls related to interest calculation for an accounting system?

A. Reperformance
B. Process walk-through
C. Observation
D. Documentation review

A is the correct answer.

Justification:
A. To ensure the effectiveness of controls, it is most effective to conduct reperformance. When the same result is obtained after the performance by an independent person, this provides the strongest assurance.
B. Process walk-through may help the auditor understand the controls better; however, it may not be as useful as conducting reperformance for a sample of transactions.
C. Observation is a valid audit method to verify that operators are using the system appropriately; however, conducting reperformance is a better method.
D. Documentation review may be of some value for understanding the control environment; however, conducting reperformance is a better method.

A1-132 Which of the following choices would be the **BEST** source of information when developing a risk-based audit plan?

A. Process owners identify key controls.
B. System custodians identify vulnerabilities.
C. Peer auditors understand previous audit results.
D. Senior management identify key business processes.

D is the correct answer.

Justification:

A. Although process owners should be consulted to identify key controls, senior management is a better source to identify business processes, which are more important.
B. System custodians is a good source to better understand the risk and controls as they apply to specific applications; however, senior management is a better source to identify business processes, which are more important.
C. The review of previous audit results is one input into the audit planning process; however, if previous audits focused on a limited or a restricted scope or if the key business processes have changed and/or new business processes have been introduced, then this does contribute to the development of a risk-based audit plan.
D. Developing a risk-based audit plan must start with the identification of key business processes, which determine and identify the risk that needs to be addressed.

A1-133 While auditing a third-party IT service provider, an IS auditor discovered that access reviews were not being performed as required by the contract. The IS auditor should:

A. Report the issue to IT management.
B. Discuss the issue with the service provider.
C. Perform a risk assessment.
D. Perform an access review.

A is the correct answer.

Justification:

A. During an audit, if there are material issues that are of concern, they need to be reported to management in the audit report.
B. The IS auditor may discuss the issue with the service provider; however, the appropriate response is to report the issue to IT management because they are ultimately responsible.
C. This issue can serve as an input for a future risk assessment, but the issue of noncompliance should be reported to management regardless of whether the IS auditor believes there is a significant risk.
D. The IS auditor could perform an access review as part of the audit to determine if there are errors, but not on behalf of the third-party IT service provider. It is more important to report the issue in the audit report to management.

A1-134 Which of the following is the **PRIMARY** requirement for reporting IS audit results? The report is:

A. Prepared according to a predefined and standard template.
B. Backed by sufficient and appropriate audit evidence.
C. Comprehensive in coverage of enterprise processes.
D. Reviewed and approved by audit management.

B is the correct answer.

Justification:

A. Preparation of the IS audit report according to a predefined and standard template may be useful in ensuring that all key aspects are provided in a uniform structure, but this does not demonstrate that audit findings are based on evidence that can be proven, if required.
B. ISACA IS audit standards require that reports should be backed by sufficient and appropriate audit evidence so that they demonstrate the application of the minimum standard of performance, and the findings and recommendations can be validated, if required.
C. The scope and coverage of IS audit is defined by a risk assessment process, which may not always provide comprehensive coverage of processes of the enterprise.
D. While from an operational standpoint an audit report should be reviewed and approved by audit management, the more critical consideration is that all conclusions are backed by sufficient and appropriate audit evidence.

A1-135 An IS auditor performing an audit of the risk assessment process should **FIRST** confirm that:

A. Reasonable threats to the information assets are identified.
B. Technical and organizational vulnerabilities have been analyzed.
C. Assets have been identified and ranked.
D. The effects of potential security breaches have been evaluated.

C is the correct answer.

Justification:

A. The threats facing each of the organization's assets should be analyzed according to their value to the organization. This occurs after identifying and ranking assets.
B. Analyzing how these weaknesses, in the absence of mitigating controls, will impact the organization's information assets occurs after the assets and weaknesses have been identified.
C. Identification and ranking of information assets (e.g., data criticality, sensitivity, locations of assets) will set the tone or scope of how to assess risk in relation to the organizational value of the asset.
D. The effect of security breaches is dependent on the value of the assets and the threats, vulnerabilities and effectiveness of mitigating controls. The impact of an attack against a weakness should be identified so that controls can be evaluated to determine if they effectively mitigate the weaknesses.

A1-136 Which of the following represents an example of a preventive control with respect to IT personnel?

A. A security guard stationed at the server room door
B. An intrusion detection system
C. Implementation of a badge entry system for the IT facility
D. A fire suppression system in the server room

C is the correct answer.

Justification:
A. A security guard is a deterrent control.
B. An intrusion detection system is a detective control.
C. **Preventive controls are used to reduce the probability of an adverse event. A badge entry system prevents unauthorized entry to the facility.**
D. A fire suppression system is a corrective control.

A1-137 Which of the following is an attribute of the control self-assessment approach?

A. Broad stakeholder involvement
B. Auditors are the primary control analysts
C. Limited employee participation
D. Policy driven

A is the correct answer.

Justification:
A. **The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training—all of which are representations of broad stakeholder involvement.**
B. IS auditors are the primary control analysts in a traditional audit approach. CSA involves many stakeholders, not just auditors.
C. Limited employee participation is an attribute of a traditional audit approach.
D. Policy-driven is an attribute of a traditional audit approach.

A1-138 An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization discovered the following:

- The existing DRP was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
- The DRP was presented to the deputy chief executive officer (CEO) for approval and formal issue, but it is still awaiting attention.
- The DRP has never been updated, tested or circulated to key management and staff, although interviews show that each would know what action to take for its area if a disruptive incident occurred.

The IS auditor's report should recommend that:

A. The deputy chief executive officer (CEO) is censured for failure to approve the plan.
B. A board of senior managers is set up to review the existing plan.
C. The existing plan is approved and circulated to all key management and staff.
D. A manager coordinates the creation of a new or revised plan within a defined time limit.

D is the correct answer.

Justification:

A. Censuring the deputy CEO will not improve the current situation and is generally not within the scope of an IS auditor to recommend.
B. Establishing a board to review the disaster recovery plan (DRP), which is two years out of date, may achieve an updated DRP but is not likely to be a speedy operation; issuing the existing DRP would be imprudent without first ensuring that it is workable.
C. The current DRP may be unacceptable or ineffective and recommending the approval of the DRP may be unwise. The best way to develop a DRP in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.
D. The primary concern is to establish a workable DRP that reflects current processing volumes to protect the organization from any disruptive incident.

A1-139 An IS auditor finds that a disaster recovery plan (DRP) for critical business functions does not cover all systems. Which of the following is the **MOST** appropriate course of action for the IS auditor?

A. Alert management and evaluate the impact of not covering all systems.
B. Cancel the audit.
C. Complete the audit of the systems covered by the existing DRP.
D. Postpone the audit until the systems are added to the DRP.

A is the correct answer.

Justification:

A. An IS auditor should make management aware that some systems are omitted from the disaster recovery plan (DRP). An IS auditor should continue the audit and include an evaluation of the impact of not including all systems in the DRP.
B. Canceling the audit is an inappropriate action.
C. Ignoring the fact that some systems are not covered would violate audit standards that require reporting all material findings and is an inappropriate action.
D. Postponing the audit is an inappropriate action. The audit should be completed according to the initial scope with identification to management of the risk of systems not being covered.

A1-140 Which of the following is **MOST** effective for monitoring transactions exceeding predetermined thresholds?

A. Generalized audit software
B. An integrated test facility
C. Regression tests
D. Transaction snapshots

A is the correct answer.

Justification:

A. **Generalized audit software (GAS) is a data analytic tool that can be used to filter large amounts of data.**
B. Integrated test facilities test the processing of the data and cannot be used to monitor real-time transactions.
C. Regression tests are used to test new versions of software to ensure that previous changes and functionality are not inadvertently overwritten or disabled by the new changes.
D. Gathering information through snapshots alone is not sufficient. GAS will assist with an analysis of the data.

A1-141 Which of the following is **MOST** important to ensure that effective application controls are maintained?

A. Exception reporting
B. Manager oversight
C. Control self-assessment
D. Peer reviews

C is the correct answer.

Justification:

A. Exception reporting only looks at errors or problems but will not ensure controls are still working.
B. Manager oversight is important but may not be a consistent or well-defined process compared to control self-assessment.
C. **CSA is the review of business objectives and internal controls in a formal and documented collaborative process. It includes testing the design of automated application controls.**
D. Peer reviews lack the direct involvement of audit specialists and management.

A1-142 The success of a control self-assessment depends highly on:

A. Line managers assuming a portion of the responsibility for control monitoring
B. Assigning staff managers, the responsibility for building controls
C. The implementation of a stringent control policy and rule-driven controls
D. The implementation of supervision and monitoring of controls of assigned duties

A is the correct answer.

Justification:

A. **The primary objective of a control self-assessment (CSA) program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a CSA program depends on the degree to which line managers assume responsibility for controls. This enables line managers to detect and respond to control errors promptly.**
B. CSA requires managers to participate in the monitoring of controls.
C. The implementation of stringent controls will not ensure controls are working correctly.
D. Better supervision is a compensating and detective control and may assist in ensuring control effectiveness but would work best when used in a formal process such as CSA.

A1-143 Which of the following is evaluated as a preventive control by an IS auditor performing an audit?

A. Transaction logs
B. Before and after image reporting
C. Table lookups
D. Tracing and tagging

C is the correct answer.

Justification:

A. Transaction logs are a detective control and provide audit trails.
B. Before and after image reporting makes it possible to trace the impact that transactions have on computer records. This is a detective control.
C. **Table lookups are preventive controls; input data are checked against predefined tables, which prevent any undefined data to be entered.**
D. Tracing and tagging is used to test application systems and controls but is not a preventive control in itself.

A1-144 Which of the following is a **PRIMARY** objective of embedding an audit module while developing online application systems?

A. To collect evidence while transactions are processed
B. To reduce requirements for periodic internal audits
C. To identify and report fraudulent transactions
D. To increase efficiency of the audit function

A is the correct answer.

Justification:

A. **Embedding a module for continuous auditing within an application processing a large number of transactions provides timely collection of audit evidence during processing and is the primary objective. The continuous auditing approach allows the IS auditor to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.**
B. An embedded audit module enhances the effectiveness of internal audit by ensuring timely availability of required evidence. It may not reduce the requirements for periodic internal audits, but it will increase their efficiency. Also, the question pertains to the development process for new application systems, and not to subsequent internal audits.
C. An audit module collects data on transactions that may help identify fraudulent transactions, but it does not identify fraudulent transactions inherently.
D. Although increased efficiency may be an added benefit of an embedded audit module, it is not the primary objective.

A1-145 An IS audit department considers implementing continuous auditing techniques for a multinational retail enterprise that requires high availability of its key systems. A **PRIMARY** benefit of continuous auditing is that:

A. Effective preventive controls are enforced.
B. System integrity is ensured.
C. Errors can be corrected in a timely fashion.
D. Fraud can be detected more quickly.

D is the correct answer.

Justification:

A. Continuous monitoring is detective in nature and, therefore, does not necessarily assist the IS auditor in monitoring for preventive controls. The approach will detect and monitor for errors that have already occurred. In addition, continuous monitoring will benefit the internal audit function in reducing the use of auditing resources and in the timely reporting of errors or inconsistencies.
B. System integrity is typically associated with preventive controls such as input controls and quality assurance reviews. These controls do not typically benefit an internal auditing function implementing continuous monitoring. Continuous monitoring benefits the internal audit function because it reduces the use of auditing resources.
C. Continuous audit will detect errors but not correct them. Correcting errors is the function of the organization's management and not the internal audit function. Continuous auditing benefits the internal audit function because it reduces the use of auditing resources to create a more efficient auditing function.
D. Continuous auditing techniques assist the auditing function in reducing the use of auditing resources through continuous collection of evidence. This approach assists the IS auditors in identifying fraud in a timely fashion and allows the auditors to focus on relevant data.

A1-146 An IS auditor wants to determine the effectiveness of managing user access to a server room. Which of the following is the **BEST** evidence of effectiveness?

A. Observation of a logged event
B. Review of the procedure manual
C. Interview with management
D. Interview with security personnel

A is the correct answer.

Justification:

A. Observation of the process to reset an employee's security access to the server room and the subsequent logging of this event provide the best evidence of the adequacy of the physical security control.
B. Although reviewing the procedure manual can be helpful in gaining an overall understanding of a process, it is not evidence of the effectiveness of the execution of a control.
C. Although interviewing management can be helpful in gaining an overall understanding of a process, it is not evidence of the effectiveness of the execution of a control.
D. Although interviewing security personnel can be helpful in gaining an overall understanding of a process, it is not evidence of the effectiveness of the execution of a control.

A1-147 As part of audit planning, an IS auditor is designing various data validation tests to effectively detect transposition and transcription errors. Which of the following will **BEST** help in detecting these errors?

A. Range check
B. Validity check
C. Duplicate check
D. Check digit

D is the correct answer.

Justification:

A. Range checks can only ensure that data fall within a predetermined range but cannot detect transposition errors.
B. Validity checks are generally programmed checking of data validity in accordance with predetermined criteria.
C. Duplicate check analysis is used to test defined or selected primary keys for duplicate primary key values.
D. A check digit is a numeric value that has been calculated mathematically and is added to data to ensure that original data have not been altered or that an incorrect, but valid, match has occurred. The check digit control is effective in detecting transposition and transcription errors.

A1-148 The **MAIN** purpose of the annual IS audit plan is to:

A. Allocate resources for audits.
B. Reduce the impact of audit risk.
C. Develop a training plan for auditors.
D. Minimize the audit costs.

A is the correct answer.

Justification:

A. Because IS audit assignments need to be accomplished with limited time and human resources, audits are scheduled and prioritized as determined by IS audit management.
B. Audit risk is inherent to all audits, and the schedule has no bearing on the impact to audit risk.
C. Developing a training plan for auditors is important, but it is not the main purpose of an IS audit plan.
D. Minimizing the audit costs could be one of the objectives of annual IS audit plan. However, this would be a result of ensuring audit resources are used effectively.

A1-149 Which of the following would be expected to approve the audit charter?

A. Chief financial officer
B. Chief executive officer
C. Audit steering committee
D. Audit committee

D is the correct answer.

Justification:

A. The chief financial officer (CFO) does not approve the audit charter but may be responsible for allocating funds in support of the audit charter. The CFO may also be a part of the audit committee or audit steering committee but would not approve the charter on their own.
B. The chief executive officer (CEO) does not approve the audit charter. The CEO may be informed, but they are independent of the audit committee.
C. The steering committee would most likely be composed of various members of senior management whose purpose is to work under the framework of the audit charter and would not approve the charter itself.
D. One of the primary functions of the audit committee is to create and approve the audit charter.

A1-150 Which of the following is the **PRIMARY** purpose of a risk-based audit?

A. High-impact areas are addressed first.
B. Audit resources are allocated efficiently.
C. Material areas are addressed first.
D. Management concerns are prioritized.

C is the correct answer.

Justification:
A. High-impact does not necessarily indicate high risk. Risk also takes into consideration probability.
B. Although a risk-based audit approach does address allocation of resources, that is not the primary function of a risk-based audit approach.
C. Material risk is audited according to the risk ranking, thus enabling the audit team to concentrate on high-risk areas first.
D. Management concerns may not be aligned with high-risk areas.

A1-151 An auditee disagrees with an audit finding. Which of the following is the **BEST** course of action for the IT auditor to take?

A. Discuss the finding with the IT auditor's manager.
B. Retest the control to confirm the finding.
C. Elevate the risk associated with the control.
D. Discuss the finding with the auditee's manager.

A is the correct answer.

Justification:
A. Discussing the disagreement with the auditor's manager is the best course of action because other actions can weaken relationships with the auditee and auditor.
B. This may unnecessarily expend human and time resources. The audit manager should determine if controls need to be retested.
C. Elevating the risk will not address the disagreement.
D. It is usually best to consult the audit manager prior to escalating the issue the auditee's manager. This could prove to be an adversarial action.