ISACA

CISA EXAM PREPARATION

ABOUT THE CISA EXAM

ISACA

WELCOME!

This program is designed to prepare you for success on the CISA exam, one step in the process of becoming certified.

The program will include:

- Information about the CISA exam and certification
- Detailed coverage of the body of knowledge required by CISA
- Activities, exam discussion questions, and group discussions
- Real-world examples of CISA subject matter

ISACA

CISA CERTIFICATION

CISA certification benefits include:

Gives you a competitive edge	Helps you achieve a high professional standard	Confirms and demonstrates your knowledge and experience
Quantifies and markets your experience	Provides global recognition as a mark of excellence	Increases your value to your organization

ISACA

CISA ACCREDITATION

The American National Standards Institute (ANSI) has accredited CISA under ISO/IEC 17024:2012, General Requirements for Bodies Operating Certification Schemes for Persons.

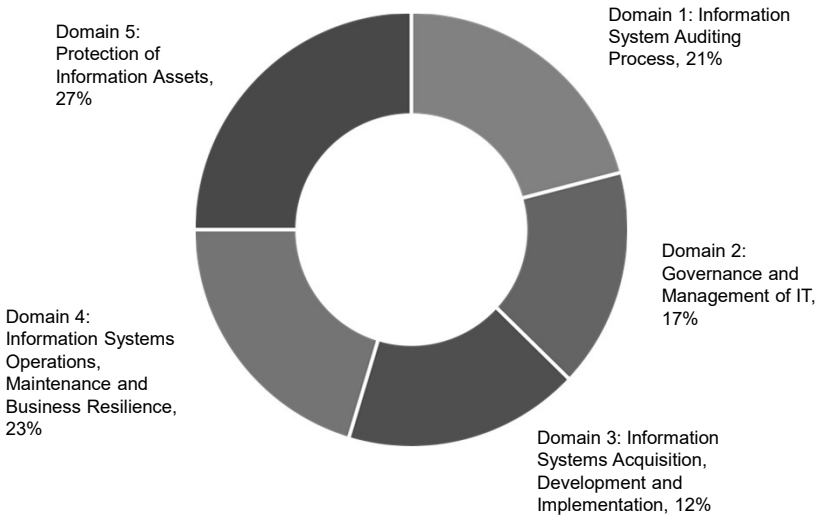
Accreditation by ANSI achieves the following:

- Promotes the unique qualifications and expertise ISACA's certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

More than 118,000 professionals have earned the CISA certification since it was introduced in 1978.

ISACA

JOB PRACTICE



ISACA

BASIS OF THE CISA EXAM

The CISA exam is based on a job practice.

Topics that candidates are expected to understand are described in a series of task and knowledge statements.

- Task statements describe the specific tasks the CISA candidate should be able to perform.
- Knowledge statements are the knowledge areas required in order for the candidate to perform the tasks.

Test questions are specifically designed to validate that the candidate possesses the knowledge to perform a given task.

ISACA

EXAM QUESTIONS

CISA exam questions are developed with the intent of measuring and testing both of the following:

- Practical knowledge
- The application of general concepts and standards

All questions are multiple-choice and are designed for one best answer from the four options given.

Scenario-based questions have the following features:

- Normally include a description of a situation
- Require you to answer two or more questions based on the information provided

ISACA

ANSWERING EXAM QUESTIONS

Read each question carefully.

Eliminate known incorrect answers.

Make the best choice possible.

Identify key words or phrases in the question (e.g., MOST, BEST or FIRST) before selecting and recording an answer.

ISACA

ANSWERING EXAM QUESTIONS (CONT'D)

Read the provided instructions carefully before attempting to answer questions.

- Skipping over these directions or reading them too quickly could result in missing important information and possibly losing credit points.

Answer all questions. There is no penalty for wrong answers.

Grading is based solely on the number of questions answered correctly.

ISACA

EXAM TIPS

Become familiar with the exact location of, and the best travel route to, the exam site prior to the date of the exam.

Arrive at the exam testing site prior to your scheduled appointment time.

- Exam candidates who are more than 15 minutes late are considered as a no-show and will forfeit their registration fee.

The exam is administered over a four-hour period, allowing for a little over 1.5 minutes per question.

ISACA

DAY OF THE EXAM

To be admitted into the test site, candidates an original government-issued ID that contains the candidate's name as it appears on their Notification to Schedule email. Acceptable forms of ID include:

- Driver's license
- State identity card (non-driver license)
- Passport
- Passport card
- Military ID
- Green card, alien registration, permanent resident card
- National identification card

Candidates who do not provide an acceptable form of identification will not be allowed to sit for the exam and will forfeit their registration fee.

ISACA

DAY OF THE EXAM (CONT'D)

To be admitted into the test site, candidates must bring the following:

- The email printout or a printout of the downloaded admission ticket
- An acceptable form of photo identification, such as a driver's license, passport or government ID
  - It must be a current and original government issued identification.
  - It must not be handwritten.
  - It must contain both the candidate's name as it appears on the admission ticket and the candidate's photograph.

Candidates who do not provide an acceptable form of identification will not be allowed to sit for the exam and will forfeit their registration fee.

ISACA

EXAM RULES

Candidates should dress to their own comfort level.

- As testing centers vary, every attempt will be made to make the climate control comfortable at each exam venue, but this cannot be guaranteed.

Do not bring reference materials, blank paper, calculators, etc.

Communication/recording devices (e.g., cell phones, tablets, smart watches, etc.) are not permitted.

No baggage of any kind is not permitted. Visit www.isaca.org for more information.

Visitors are not permitted at the testing center.

No food or beverages are allowed.

ISACA

EXAM RULES (CONT'D)

Candidates must gain authorization by a test proctor to leave the testing area. The proctor will pause the exam whenever a candidate leaves the testing station or an interruption occurs. If the reason for the interruption is not confirmed as an emergency, the test will end.

Candidates may leave the testing area with authorization during the examination to visit the facilities. Candidates will be required to check-out and check-in again upon re-entering the testing area. Note the examination time will not stop and no extra time will be allotted.

ISACA

EXAM SCORING

Candidate scores are reported as a scaled score.

- A scaled score is a conversion of a candidate's raw score on the exam to a common scale.
- ISACA uses and reports scores on a common scale from 200 to 800.

To pass, a candidate must receive a score of 450 or higher, which represents a minimum consistent standard of knowledge as established by ISACA's CISA Certification Working Group.

ISACA

THE SCORE REPORT

You will receive a preliminary score at the end of the exam.

Official scores will be sent via email within 10 days.

ISACA

THE SCORE REPORT (CONT'D)

Each candidate who completes the CISA exam will receive a score report.

- This score report contains a sub-score for each job practice domain.
- These can be useful in identifying those areas in which further study may be needed, should retaking the exam be necessary.

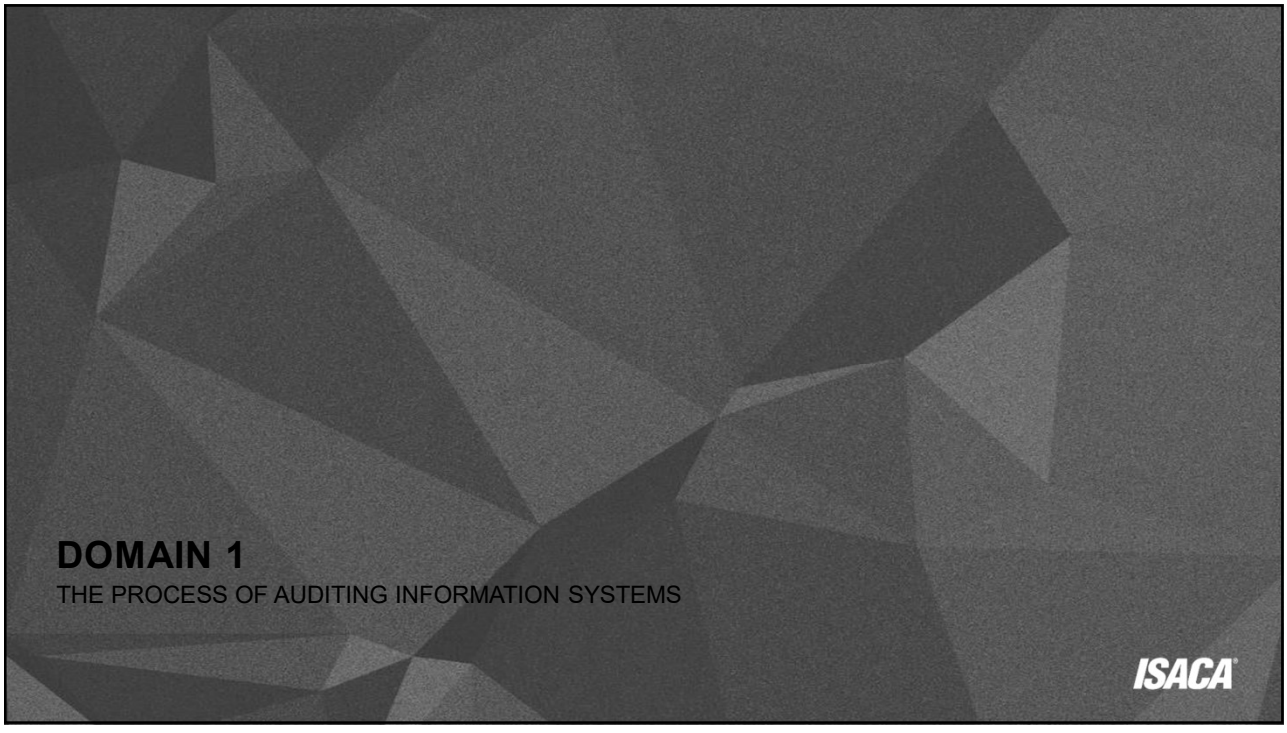
ISACA

CERTIFICATION STEPS

To earn the CISA designation, the CISA candidate must meet the following requirements:

- Pass the CISA exam.
- Submit an application (within five years of the exam passing date) with verified evidence of a minimum of at least five years of cumulative work experience performing the tasks of a CISA professional.
- Adhere to the ISACA Code of Professional Ethics.
- Agree to comply with the CISA continuing education policy.
- Comply with the Information Systems Auditing Standards.

ISACA



DOMAIN 1 OVERVIEW

The information systems (IS) auditing process encompasses the standards, principles, methods, guidelines, practices and techniques that an IS auditor uses to plan, execute, assess and review business or information systems and related processes.

An IS auditor must have a thorough understanding of this auditing process as well as IS processes, business processes and controls designed to achieve organizational objectives and protect organizational assets.

ISACA

DOMAIN 1 OBJECTIVES

Upon completion of this domain an IS auditor should be able to:

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Conduct an audit in accordance with IS audit standards and a risk-based IS audit strategy.
- Communicate audit progress, findings, results, and recommendations to stakeholders.
- Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organization's IT policies and practices.

DOMAIN 1 TOPICS

Planning

- IS Audit Standards, Guidelines and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments

Execution

- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques
- Quality Assurance and Improvement of the Audit Process

ISACA

ISACA

PLANNING

SECTION 1

TOPICS

Introduction

IS Audit Standards, Guidelines and Codes of Ethics

Business Processes

Types of Controls

Risk Based Audit Planning

25

WHAT IS AUDIT?

IS audit is the formal examination and/or testing of information systems to determine whether:

- Information systems (IS) are in compliance with applicable laws, regulations, contracts and/or industry guidelines.
- Information systems and related processes comply with governance criteria and related and relevant policies and procedures.
- IS data and information have appropriate levels of confidentiality, integrity and availability.
- IS operations are accomplished efficiently and effectiveness targets are met.

26

ISACA

AUDIT PROCESS

ISACA

IS AUDIT STANDARDS, GUIDELINES, AND CODES OF ETHICS

SECTION 1

ISACA

ISACA IS AUDIT AND ASSURANCE STANDARDS

ISACA IS audit and assurance standards define mandatory requirements for IS auditing and reporting and inform:

- IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the CISA designation of their professional performance requirements

ISACA

ISACA IS AUDIT AND ASSURANCE STANDARDS FRAMEWORK

The framework for the ISACA IS Audit and Assurance Standards provides for multiple levels of documents:

- Standards define mandatory requirements for IS audit and assurance and reporting.
- Guidelines provide guidance in applying IS audit and assurance standards. The IS auditor should consider them in determining how to achieve implementation of the above standards, use professional judgment in their application and be prepared to justify any departure from the standards.
- Tools and techniques provide examples of processes an IS auditor might follow in an audit engagement. The tools and techniques documents provide information on how to meet the standards when completing IS auditing work, but do not set requirements.

ISACA

STANDARDS AND GUIDELINES

There are three categories of standards and guidelines:

Category	Description
General (Guiding principles)	Apply to the conduct of all assignments, and deal with ethics, independence, objectivity and due care as well as knowledge, competency and skill
Performance	Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence
Reporting	Address the types of reports, means of communication and the information communicated

ISACA

ISACA IS AUDIT AND ASSURANCE GUIDELINES

Consider them in determining how to implement ISACA audit and assurance standards.

Use professional judgment in applying them to specific audits.

Be able to justify any departure from the ISACA audit and assurance standards.

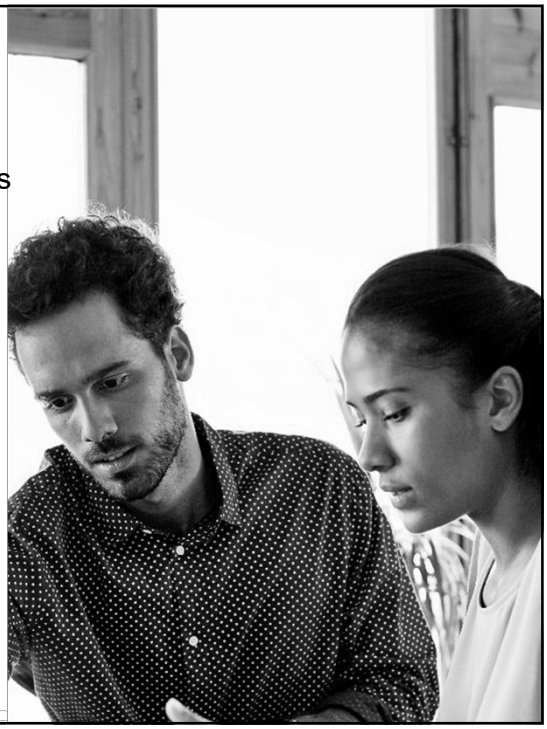
ISACA

CODE OF PROFESSIONAL ETHICS

Support the implementation of, and encourage compliance with, appropriate standards, procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.

Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the association.



CODE OF PROFESSIONAL ETHICS (CONT'D)

Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

Maintain competency in their respective fields, and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

CODE OF PROFESSIONAL ETHICS (CONT'D)

Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security and risk management.

ITAF

ITAF is a comprehensive and good practice-setting reference model that:

- Establishes standards that address IS auditor roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements.
- Defines terms and concepts specific to IS assurance.
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments.

BUSINESS PROCESSES

37

ISACA

OVERVIEW

IS auditor's key actions

- Understand and evaluate business process
- Test and evaluate operational controls
- Identify the controls:
  - Policies
  - Procedures
  - Practices
  - Organizational structures

38

TOPICS

IS Internal Audit Function

Management of the IS Audit Function

Audit Planning

Effect of Laws and Regulations on IS Audit Planning

Business Process Applications and Controls

39

IS INTERNAL AUDIT FUNCTION

The role of the IS internal audit function should be established by an audit charter approved by the board of directors and the audit committee (senior management if these entities do not exist).

An audit charter is an overarching document that covers the entire scope of audit activities in an entity while an engagement letter is more focused on a particular audit exercise that is sought to be initiated in an organization with a specific objective in mind.

The charter should clearly state management's responsibility and objectives for, and delegation of authority to, the IS audit function.

40

ISACA

MANAGEMENT OF THE IS AUDIT FUNCTION

Managing the IS audit function should ensure value-added contributions to senior management in the efficient management of IT and achievement of business objectives.

41

AUDIT PLANNING

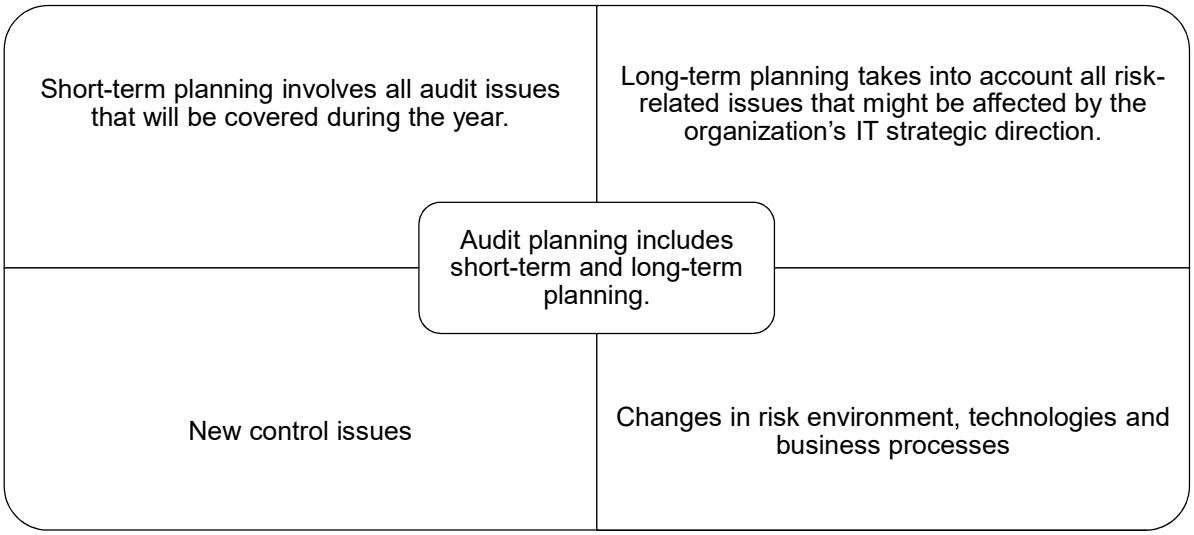
The first step in performing an IS audit is adequate planning.

To plan an audit, the following tasks must be completed:

- List all the processes that may be considered for the audit.
- Evaluate each process by performing a qualitative or quantitative risk assessment.
  - These evaluations should be based on objective criteria.
- Define the overall risk of each process.
- Construct an audit plan to include all of the processes that are rated “high” which would represent the ideal annual audit plan.

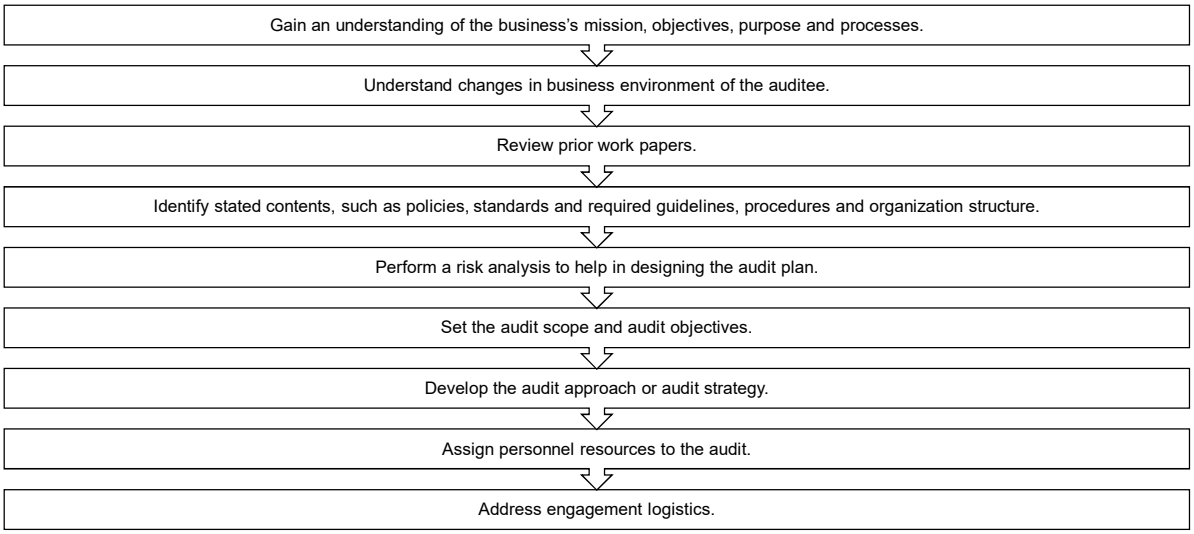
ISACA

WHEN TO AUDIT



ISACA

AUDIT PLANNING STEPS



ISACA

ADDITIONAL CONSIDERATIONS

The audit plan should take into consideration the objectives of the IS audit relevant to the audit area and its technology infrastructure and business strategic direction. The IS auditor can gain this information by:

- Reading background material, including industry publications, annual reports and independent financial analysis reports
- Reviewing prior audit reports or IT-related reports (from external or internal audits, or specific reviews such as regulatory reviews)
- Reviewing business and IT long-term strategic plans

ISACA

ADDITIONAL CONSIDERATIONS (CONT'D)

Other ways the IS auditor can gain this information include:

- Interviewing key managers to understand business issues
- Identifying specific regulations applicable to IT
- Identifying IT functions or related activities that have been outsourced
- Touring key organization facilities

The IS auditor must also match available audit resources, such as staff, with the tasks defined in the audit plan.

ISACA

LAWS AND REGULATIONS

Certain industries, such as banks and internet service providers (ISPs), are closely regulated. These legal regulations may pertain to financial, operational and IS audit functions.

There are two areas of concern that impact the audit scope and objectives:

- Legal requirements placed on the audit
- Legal requirements placed on the auditee and its systems, data management, reporting, etc.

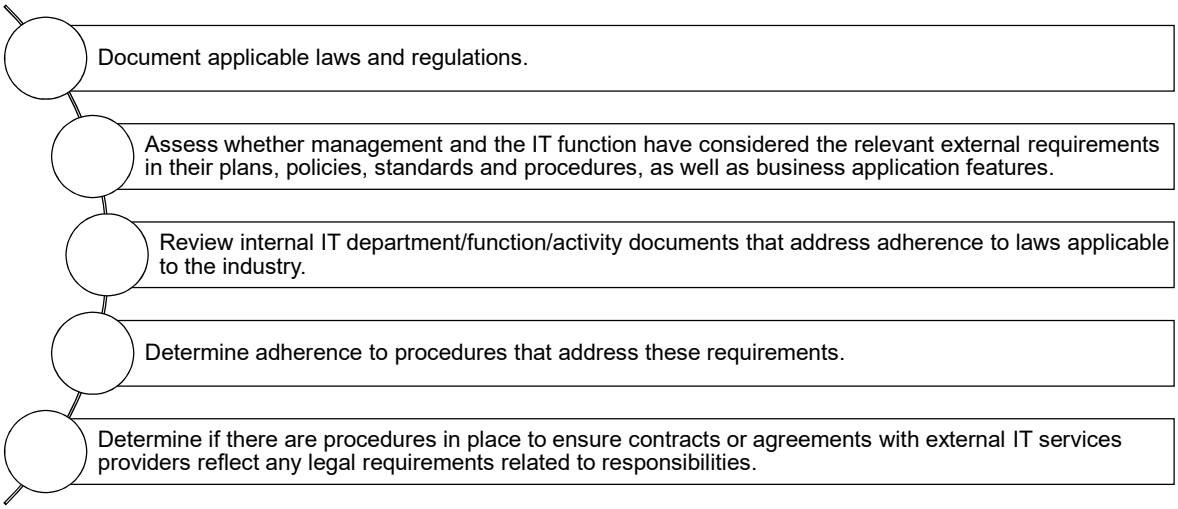
IS AUDIT ROLE AND COMPLIANCE

To determine an organization's level of compliance, an IS auditor must:

- Identify those government or other relevant external requirements dealing with:
  - Electronic data, personal data, copyrights, e-commerce, e-signatures, etc.
  - Computer system practices and controls
  - The manner in which computers, programs and data are stored
  - The organization or the activities of information technology services
  - IS audits

ISACA

IS AUDIT STEPS AND DETERMINING ORGANIZATIONAL COMPLIANCE



ISACA

BUSINESS PROCESS APPLICATIONS AND CONTROLS

In an integrated application environment, controls are embedded and designed into the business application that supports the processes. Business process control assurance involves evaluating controls at the process and activity level.

These controls may be a combination of:

- Management
- Programmed
- Manual controls

To effectively audit business application systems, an IS auditor must obtain a clear understanding of the application system under review.

50

ISACA

BUSINESS APPLICATION SYSTEMS

- E-commerce
- Electronic data interchange
- Email
- Point-of-sale (POS) systems
- Electronic banking and electronic finance
- Payment systems and electronic funds transfer (EFT)
- Automated teller machines (ATM)
- Supply chain management (SCM)
- Purchase accounting systems
- Integrated manufacturing systems
- Industrial control systems (ICS)
- Interactive voice response (IVR)
- Image processing
- Artificial intelligence (AI) and business intelligence systems
- Decision support system (DSS)
- Customer relationship management (CRM)

ISACA

USING THE SERVICES OF OTHER AUDITORS AND EXPERTS

When using external or outside experts consider the following:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts
- Professional competence, qualifications and experience
- Scope of work proposed to be outsourced and approach
- Supervisory and audit management controls

52

ISACA

ACTIVITY

You have been assigned to an integrated audit of payroll processes and need to plan the IT audit portion of the engagement.

What is the **MOST** important business process area that you need to consider?

To help you perform the audit, would it be better to know the IS audit budget or to know the CIO and CFO risk profile for payroll processes?

DISCUSSION QUESTION

Due to resource constraints of the IS audit team, the audit plan as originally approved cannot be completed. Assuming that 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.

DISCUSSION QUESTION

Although management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should **FIRST**:

A. include the statement from management in the audit report.
B. verify the software is in use through testing.
C. include the item in the audit report.
D. discuss the issue with senior management because it could have a negative impact on the organization.

TYPES OF CONTROLS

56

ISACA

INTERNAL CONTROLS

Internal controls are normally composed of policies, procedures, practices and organizational structures that are implemented to reduce risk to the organization.

Internal controls should address:

- What should be achieved?
- What should be avoided?

ISACA

CONTROL CLASSIFICATION

Class	Function
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors).
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.

ISACA

CONTROL OBJECTIVES AND CONTROL MEASURES

Control objective

- An objective of one or more operational area(s) or role(s) to be achieved, in order to contribute to the fulfillment of strategic goal(s) of the company. That is, the control objective is such a goal, that is explicitly related to the strategy of the company.

Control measure

- An activity contributing to the fulfillment of a control objective. Both the control objective and control measure serve the decomposition of the strategic-level goals into such lower-level goals and activities, that can be assigned as tasks to the staff. This assignment can take the form of a role description in a job description.

ISACA

IS CONTROL OBJECTIVES

IS control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process area. IS control objectives are:

- Statements of the desired result or purpose to be achieved by implementing controls around information systems processes.
- Comprised of policies, procedures, practices and organizational structures.
- Designed to provide reasonable assurance that business objectives will be achieved, and undesired events will be prevented or detected and corrected.

ISACA

IS CONTROL OBJECTIVES (CONT'D)

- Safeguarding assets
- System development life cycle (SDLC) processes are established, in place and operating effectively
- Integrity of general operating system (OS) environments
- Integrity of sensitive and critical application system environments
- Appropriate identification and authentication of users
- The efficiency and effectiveness of operations
- Integrity and reliability of systems by implementing effective change management procedures
- Complying with the users' requirements, organizational policies and procedures, and applicable laws and regulations (compliance objectives)
- Ensuring availability of IT services by developing efficient business continuity plans (BCPs), disaster recovery plans (DRPs), that include backup and recovery processes
- Enhancing protection of data and systems by developing an incident response plan
- Ensuring integrity and reliability of systems by implementing effective change management procedures
- Ensuring that outsourced IS processes and services have clearly defined service level agreements (SLAs) and contract terms and conditions to ensure the organization's assets are properly protected and meet business goals and objectives

ISACA

GENERAL CONTROLS

General controls include:

- Internal accounting controls that concern the safeguarding of assets and reliability of financial information
- Operational controls that concern day-to-day operations, functions and activities
- Administrative controls that concern operational efficiency in a functional area and adherence to management policies
- Organizational security policies and procedures to ensure proper usage of assets
- Overall policies for the design and use of adequate documents and records
- Access and use procedures and practices
- Physical and logical security policies for all facilities

ISACA

IS-SPECIFIC CONTROLS

Each general control can be translated into an IS-specific control. The IS auditor should understand IS controls and how to apply them in planning an audit.

IS control procedures include:

- Strategy and direction of the IT function
- General organization and management of the IT function
- Access to IT resources, including data and programs
- Systems development methodologies and change control

ISACA

IS-SPECIFIC CONTROLS (CONT'D)

Additional IS control procedures include:

- Operations procedures
- Systems programming and technical support functions
- Quality assurance (QA) procedures
- Physical access controls
- Business continuity planning (BCP)/disaster recovery planning (DRP)
- Networks and communications
- Database administration
- Protection and detective mechanisms against internal and external attacks

ISACA

RISK-BASED AUDIT PLANNING

65

ISACA

RISK-BASED AUDITING

Gather Information and Plan

- Knowledge of business and industry
- Prior year's audit results
- Recent financial information
- Regulatory statutes
- Inherent risk assessments

Obtain Understanding of Internal Control

- Control environment
- Control procedures
- Detection risk assessment
- Control risk assessment
- Equate total risk

Perform Compliance Tests

- Identify key controls to be tested.
- Perform tests on reliability, risk prevention and adherence to organization policies and procedures.

Perform Substantive Tests

- Analytical procedures
- Detailed tests of account balances
- Other substantive audit procedures

Conclude the Audit

- Create recommendations.
- Write the audit report.

ISACA

AUDIT RISK AND MATERIALITY

Inherent risk	Control risk	Detection risk	Overall audit risk
• As it relates to audit risk, it is the risk level or exposure of the process/entity to be audited without considering the controls that management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.	• The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed due to the volume of logged information. The control risk associated with computerized data validation procedures is ordinarily low if the processes are consistently applied.	• The risk that material errors or misstatements that have occurred will not be detected by an IS auditor.	• The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under scrutiny so the overall audit risk is at a sufficiently low level at the completion of the examination.

ISACA

RISK ASSESSMENT

A risk assessment assists the IS auditor in identifying risk and threats to an IT environment and IS system, and it helps in the evaluation of controls.

Risk assessments should identify, quantify and prioritize risk against criteria for risk acceptance and objectives relevant to the organization.

It supports risk-based audit decision making by considering variables, such as:

- Technical complexity
- Level of control procedures in place
- Level of financial loss

ISACA

RISK RESPONSE

Risk Response Options

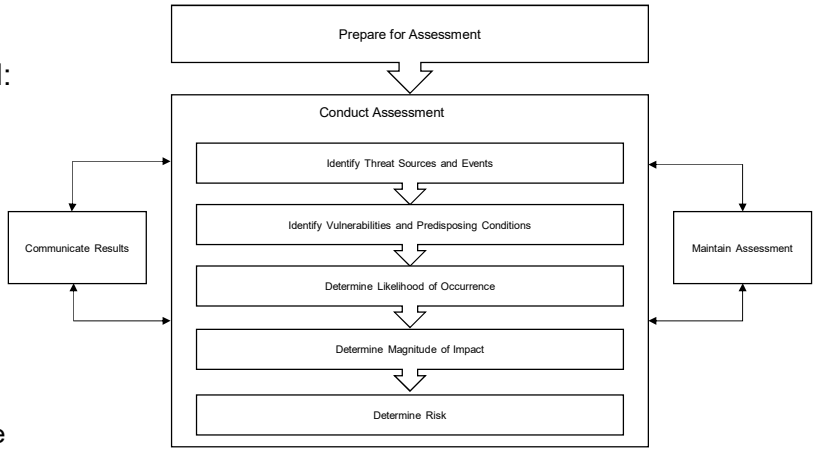
- **Risk mitigation** – Applying appropriate controls to reduce the risk
- **Risk acceptance** – Knowingly and objectively not taking action, providing the risk clearly satisfies the organization's policy and criteria for risk acceptance
- **Risk avoidance** – Avoiding risk by not allowing actions that would cause the risk to occur
- **Risk transfer/sharing** – Transferring the associated risk to other parties

ISACA

RISK ASSESSMENT PROCESS

Using risk assessment to determine areas to be audited:

- Enables management to effectively allocate limited audit resources
- Ensures that relevant information has been obtained from all levels of management
- Establishes a basis for effectively managing the audit department
- Provides a summary of how the individual audit subject is related to the overall organization as well as to the business plans



Source: National Institute of Standards and Technology (NIST), *NIST Special Publication 800-30, Revision 1: Information Security, USA, 2012.* Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

ISACA

RISK ANALYSIS

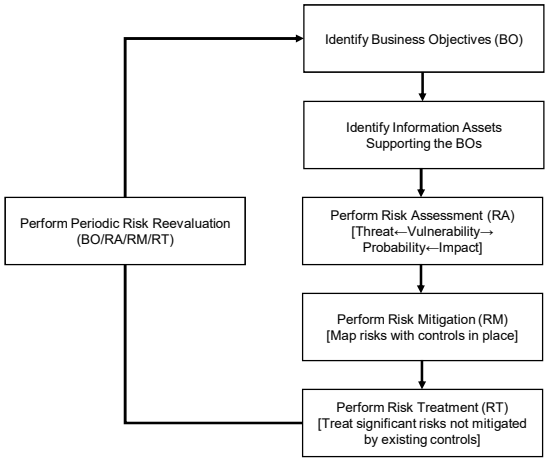
During audit planning, the IS auditor must perform or review a risk analysis to identify risks and vulnerabilities in order to determine the controls needed to mitigate those risks.

The IS auditor's role is to:

- Understand the relationship between risk and control.
- Identify and differentiate risk types and the controls used to mitigate the risk.
- Evaluate risk assessment and management techniques used by the organization.
- Understand that risk exists as part of the audit process.

ISACA

RISK MANAGEMENT PROCESS



ISACA

TYPES OF AUDITS

Type	Description
Compliance audits	Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. Examples include Payment Card Industry Data Security Standard (PCI DSS) audits for companies that process credit card data and Health Insurance Portability and Accountability Act (HIPAA) audits for companies that handle health care data.
Financial audits	The purpose of a financial audit is to assess the accuracy of financial reporting. It often involves detailed, substantive testing, although increasingly, auditors are placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.

ISACA

TYPES OF AUDITS (CONT'D)

Type	Description
Operational audits	An operational audit is designed to evaluate the internal control structure in a given process or area. Examples include IS audits of application controls or logical security systems.
Administrative audits	These are oriented to assess issues related to the efficiency of operational productivity within an organization.
IS audits	This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, and consume resources efficiently. Also, do they have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner.

ISACA

TYPES OF AUDITS (CONT'D)

Type	Description
Forensic audits	Forensic auditing has been defined as auditing specialized in discovering, disclosing and following up on fraud and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities.
Integrated audits	An integrated audit combines financial and operational audit steps. It is performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance.

ISACA

INTEGRATED AUDIT

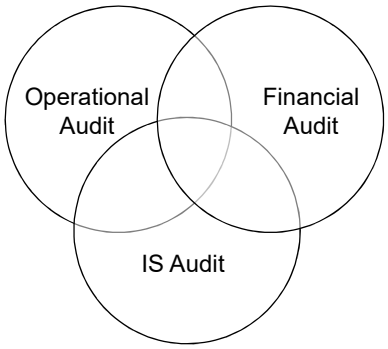
An integrated audit focuses on risk. It involves a team of auditors with different skill sets working together to provide a comprehensive report.

ISACA

INTEGRATED AUDIT (CONT'D)

The process typically involves:

- Identification of risk faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risk, design and weaknesses



ISACA

CONTINUOUS AUDITING

Continuous auditing is characterized by the short time lapse between the audit, the collection of evidence and the audit reporting.

It results in better monitoring of financial issues, such as fraud, ensuring that real-time transactions benefit from real-time monitoring.

Continuous auditing should be independent of continuous controls and continuous monitoring.

CONTINUOUS AUDITING AND MONITORING

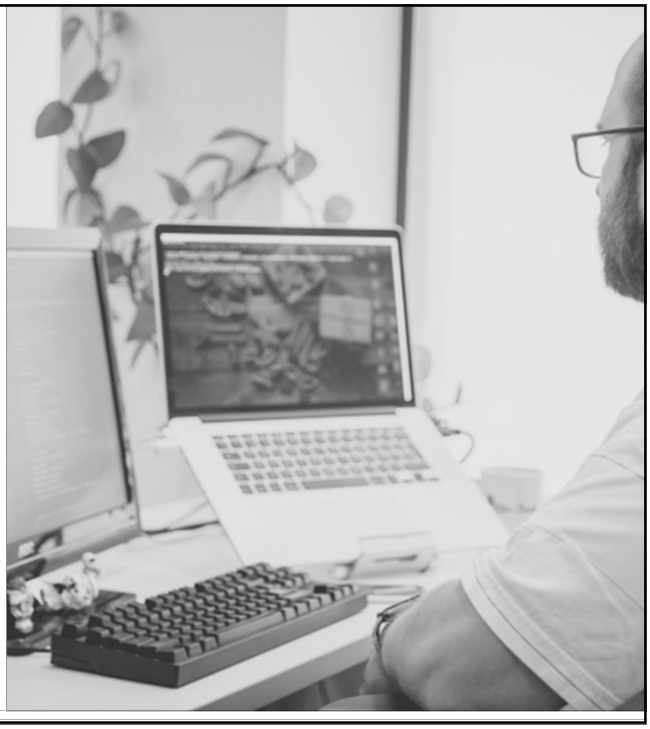
Continuous auditing	Continuous monitoring
• Continuous auditing enables an IS auditor to perform tests and assessments in a real-time or near real-time environment. Continuous auditing is designed to enable an IS auditor to report results on the subject matter being audited within a much shorter timeframe than under a traditional audit approach.	• Continuous monitoring is used by an organization to observe the performance of one or many processes, systems or types of data. For example, real-time antivirus or IDSs may operate in a continuous monitoring fashion.

ISACA

CONTINUOUS AUDITING PROCESS APPLICATIONS

This process must be carefully built into the business applications and may include IT techniques such as:

- Transaction logging
- Query tools
- Statistics and data analysis (CAAT)
- Database management systems (DBMS)
- Intelligent agents



CONTINUOUS AUDITING (CONT'D)

For continuous auditing to succeed, it needs to have:

- A high degree of automation.
- Alarm triggers to report timely control failures.
- Implementation of highly automated audit tools that require the IS auditor to be involved in setting up the parameters.
- The ability to quickly inform IS auditors of the results of automated procedures, particularly when the process has identified anomalies or errors.
- Quick and timely issuance of automated audit reports.
- Technically proficient IS auditors.
- Availability of reliable sources of evidence.
- Adherence to materiality guidelines.

ISACA

AUDIT METHODOLOGY

An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit programs.

Each audit department should design and approve an audit methodology that is formalized and communicated to all audit staff.

An audit program should be developed to serve as a guide for performing and documenting all of the audit steps, and the extent and types of evidential matter reviewed.

AUDIT PHASES

Audit Phase	Description
Audit subject	• Identify the area to be audited.
Audit objective	• Identify the purpose of the audit.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review, such as functional flow charts, policies, standards, procedures and prior audit work papers. • Identify locations or facilities to be audited. • Develop a communication plan at the beginning of each engagement that describes who to communicate to, when, how often and for what purpose(s).

ISACA

AUDIT PHASES (CONT'D)

Audit Phase	Description
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	• Identify methods (including tools) to perform the evaluation. • Identify criteria for evaluating the test (similar to a test script for the IS auditor to use in conducting the evaluation). • Identify means and resources to confirm the evaluation was accurate (and repeatable, if applicable).

ISACA

AUDIT PHASES (CONT'D)

Audit Phase	Description
Procedures for communication with management	• Determine frequency of communication. • Prepare documentation for final report.
Audit report preparation	• Disclose follow-up review procedures. • Disclose procedures to evaluate/test operational efficiency and effectiveness. • Disclose procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

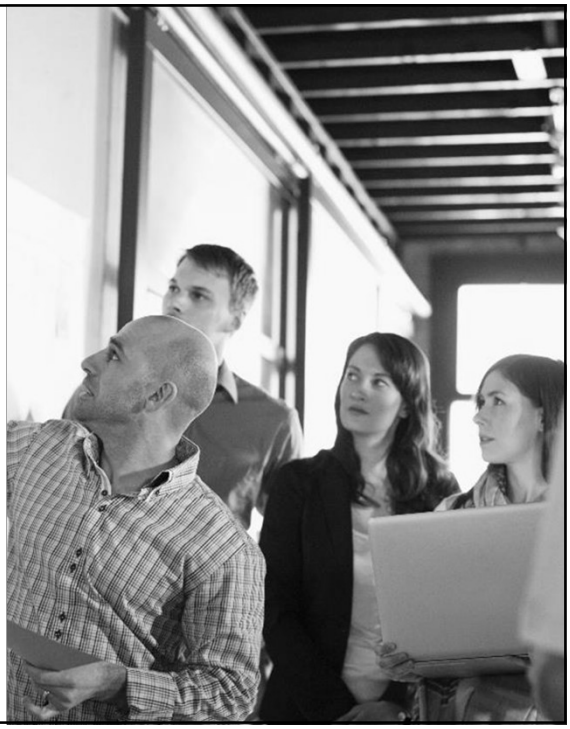
ISACA

ACTIVITY

You are planning an upcoming regulatory readiness audit for your organization. The organization has international operations, and data is fed into several legacy financial systems.

What type of audit approach do you think would be the best to perform for this IS audit?

What type of control would you use as the primary control to ensure only sales data is sent to the financial systems connected to the PCI environment?



DISCUSSION QUESTION

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:

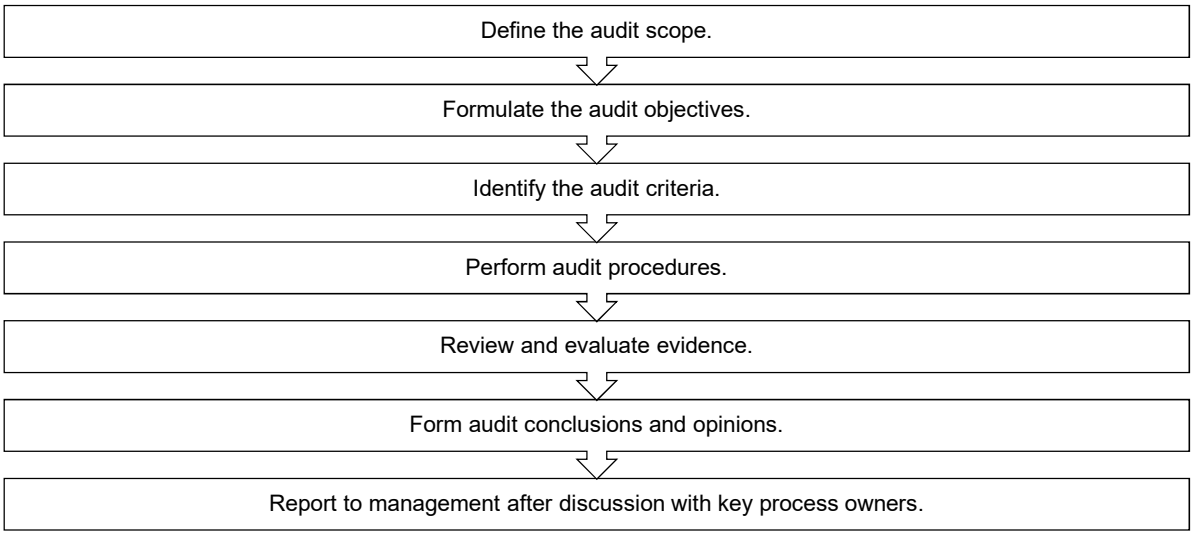
A. lower confidence coefficient, resulting in a smaller sample size.
B. higher confidence coefficient, resulting in a smaller sample size.
C. higher confidence coefficient, resulting in a larger sample size.
D. lower confidence coefficient, resulting in a larger sample size.

ISACA

EXECUTION

88

IS AUDIT STEPS



ISACA

IS AUDIT PROJECT MANAGEMENT

Plan the audit engagement.

- Plan the audit considering project-specific risk.

Build the audit plan.

- Chart the necessary audit tasks across a time line, optimizing resource use. Make realistic estimates of the time requirements for each task with proper consideration given to the availability of the auditee.

Execute the plan.

- Execute audit tasks against the plan.

Monitor project activity.

- IS auditors report their actual progress against planned audit steps to ensure challenges are managed proactively and the scope is completed within time and budget.

ISACA

INTERNAL VS. EXTERNAL AUDITS

Internal Audit	External Audit
• The scope and objectives of the audit function within the organization and are not specific to a particular IS audit.	• The scope and objectives of the audit are documented in a formal contract or statement of work.

- The **audit charter** is a document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity. It must be approved by the highest level of management or the audit committee.
- An **engagement letter** is a formal document which defines an IS auditor's responsibility, authority and accountability for a specific assignment. It does not replace an audit charter.

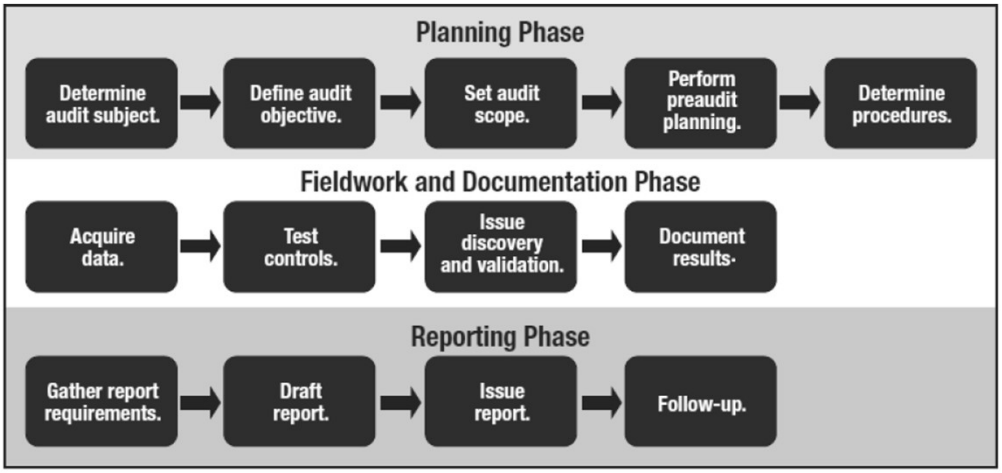
ISACA

AUDIT OBJECTIVES

A key element in IS audit planning is translating basic audit objectives into specific IS audit objectives.

Audit objectives refer to the specific goals that must be accomplished by the audit. They are often focused on validating that internal controls exist and are effective at minimizing business risk.

AUDIT PHASES



93

ISACA

AUDIT PROGRAMS

An audit program is a step-by-step set of audit procedures and instructions that should be performed to complete an audit.

Audit programs are based on the scope and objective of the particular assignment.

It is the audit strategy and plan.

It identifies scope, audit objectives and audit procedures to obtain sufficient, relevant and reliable evidence to draw and support audit conclusions and opinions.

ISACA

PROGRAM PROCEDURES

General Audit Procedures
• Obtaining and recording an understanding of the audit area/subject • A risk assessment and general audit plan and schedule • Detailed audit planning • Preliminary review of the audit area/subject • Evaluating the audit area/subject • Verifying and evaluating the appropriateness of controls designed to meet control objectives • Compliance testing • Substantive testing • Reporting • Follow-up

Procedures for Testing and Evaluating IS Controls
• The use of generalized audit software to survey the contents of data files (including system logs) • The use of specialized software to assess the contents of OS database and application parameter files • Flow-charting techniques for documenting automated applications and business processes • The use of audit logs/reports available in operation/application systems • Documentation review • Inquiry and observation • Walk-throughs • Reperformance of controls

ISACA

AUDIT WORKPAPERS

All audit plans, programs, activities, tests, findings and incidents should be properly documented in work papers.

Work papers should provide a seamless transition—with traceability and support for the work performed—from objectives to report and from report to objectives.

96

FRAUD, IRREGULARITIES AND ILLEGAL ACTS

The presence of internal controls does not altogether eliminate fraud.

An IS auditor should:

- Observe and exercise due professional care in all aspects of their work.
- Be alert to the possible opportunities that allow fraud to materialize.
- Be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT-enabled environment.
- Have knowledge of fraud and fraud indicators and be alert to the possibility of fraud and errors while performing an audit.

For additional guidance, please see standard 1207 Irregularity and Illegal Acts and guideline 2207 Irregularity and Illegal Acts.

ISACA

SAMPLING METHODOLOGY

98

ISACA

TESTING METHODS

Compliance testing:

- Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.

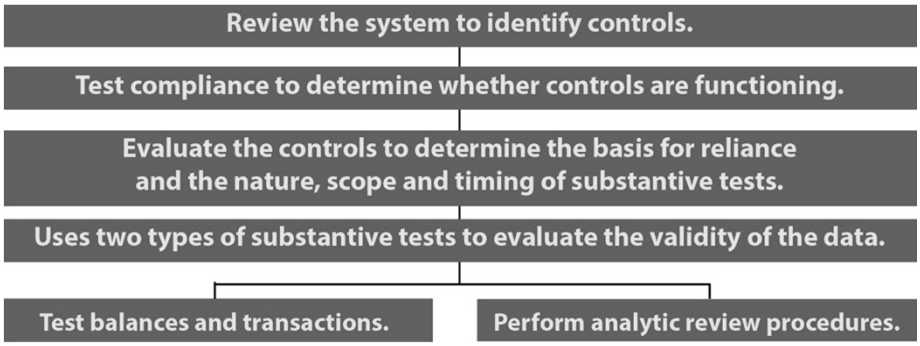
Substantive testing:

- Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.

ISACA

TESTING PROCESS

This figure shows the relationship between compliance and substantive testing and describes the two categories of substantive tests.



ISACA

SAMPLING

Sampling is used when time and cost constrain the ability to test all transactions or events.

There are two approaches to sampling:

- Statistical sampling uses an objective method to determine the sample size and selection criteria.
- Non-statistical sampling uses the IS auditor's judgment to determine the sample size and selection criteria.

ISACA

SAMPLING METHODS

Attribute sampling

- Deals with the presence or absence of an attribute
- Expressed in rates of incidence
- Generally used in compliance testing

Proportional

- Attribute sampling
- Stop-or-go sampling
- Discovery sampling

ISACA

SAMPLING METHODS (CONT'D)

Variable sampling

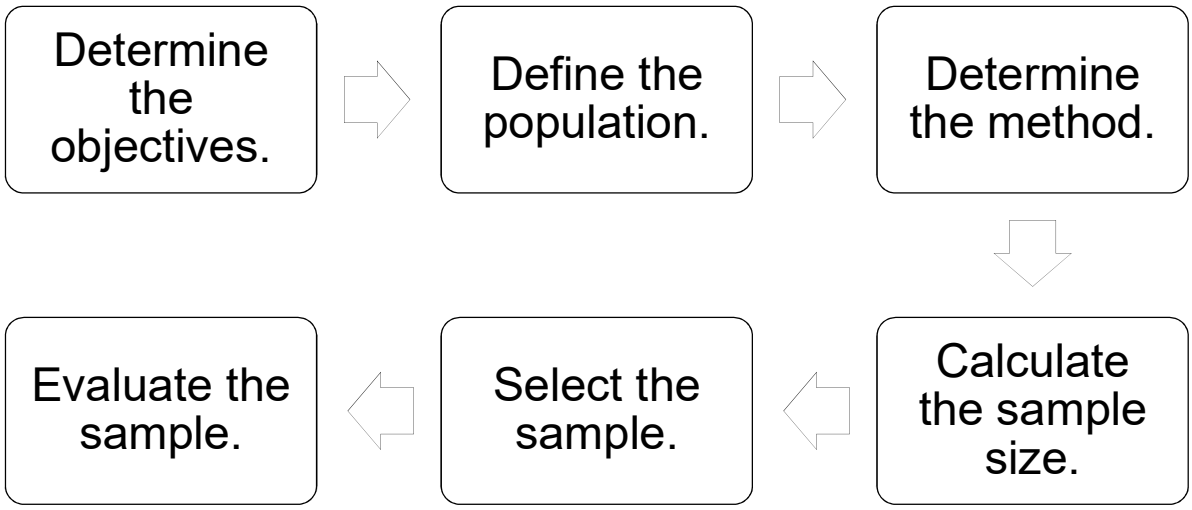
- Deals with population characteristics that vary, such as monetary values and weights
- Provides conclusions related to deviations from the norm
- Generally used in substantive testing

Variable

- Stratified mean per unit
- Unstratified mean per unit
- Difference estimation

ISACA

SAMPLING STEPS



ISACA

DISCUSSION QUESTION

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

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

AUDIT EVIDENCE COLLECTION TECHNIQUES

106

ISACA

EVIDENCE

Evidence is any information used by the IS auditor to determine whether the entity or data being audited follows the established criteria or objectives and supports audit conclusions.

Some types of evidence are more reliable than others. Reliability is determined by:

- The independence of the evidence provider
- The qualifications of the evidence provider
- The objectivity of the evidence
- The timing of the evidence

The IS auditor must focus on the objectives of the audit and not on the nature of the evidence.

Evidence is considered competent when it is both valid and relevant.

ISACA IS Audit and Assurance Standard 1205 Evidence

ISACA

EVIDENCE GATHERING TECHNIQUES

Review IS organizational structures.	Review IS policies and procedures.	Review IS standards.	Review IS documentation.
Interview appropriate personnel.	Observe processes and employee performances.	Conduct a reperformance.	Conduct walkthroughs.

ISACA

INTERVIEWS AND OBSERVATIONS

Observing personnel in the performance of their duties assists an IS auditor in identifying:

Actual functions	Actual processes/ procedures	Security awareness	Reporting relationships

- Note that personnel may change their behavior if they know they are being observed. Therefore, combine observations with interviews, which can provide adequate assurance that personnel have the required technical skills.

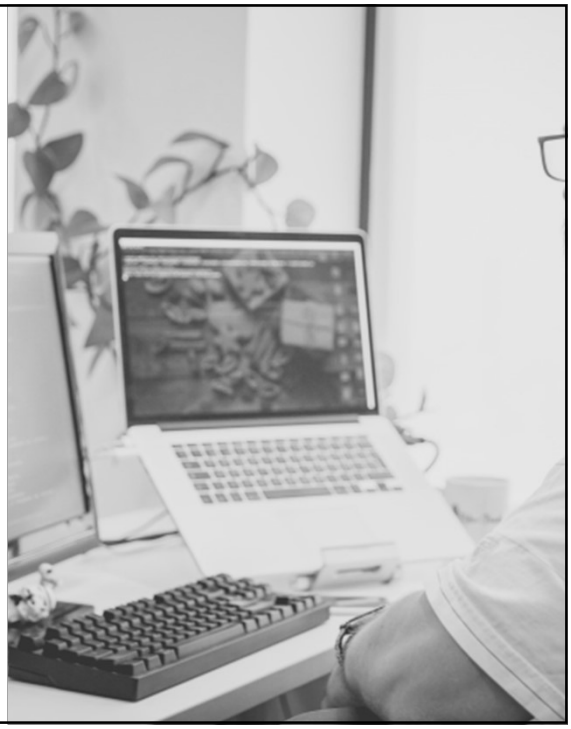
ISACA

ACTIVITY

You are assigned to perform an IS audit of user provisioning processes within the financial system of your organization that is publicly traded.

The external auditor has performed testing to meet Sarbanes-Oxley requirements. What do you think would be the **BEST** course of action to scope this IT audit?

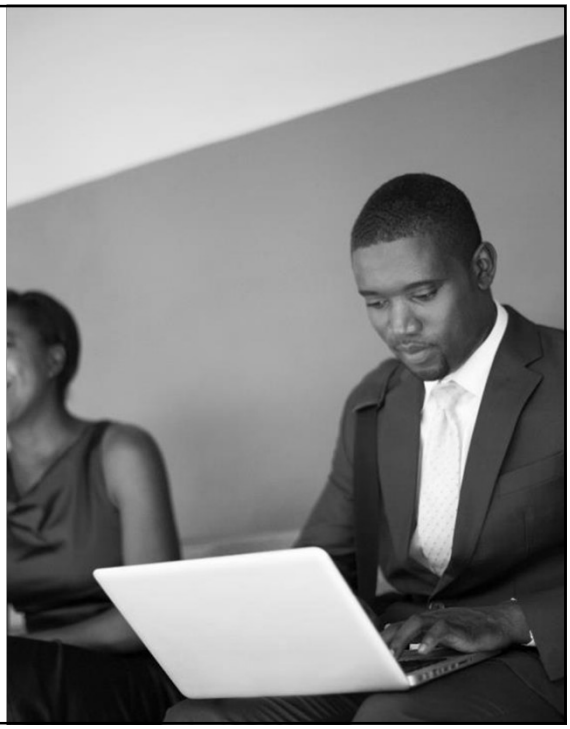
During the planning of your IT audit, the process owner identifies an area that needs improvement. What additional quality systems techniques would best suit this type of assessment?



DISCUSSION QUESTION

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?

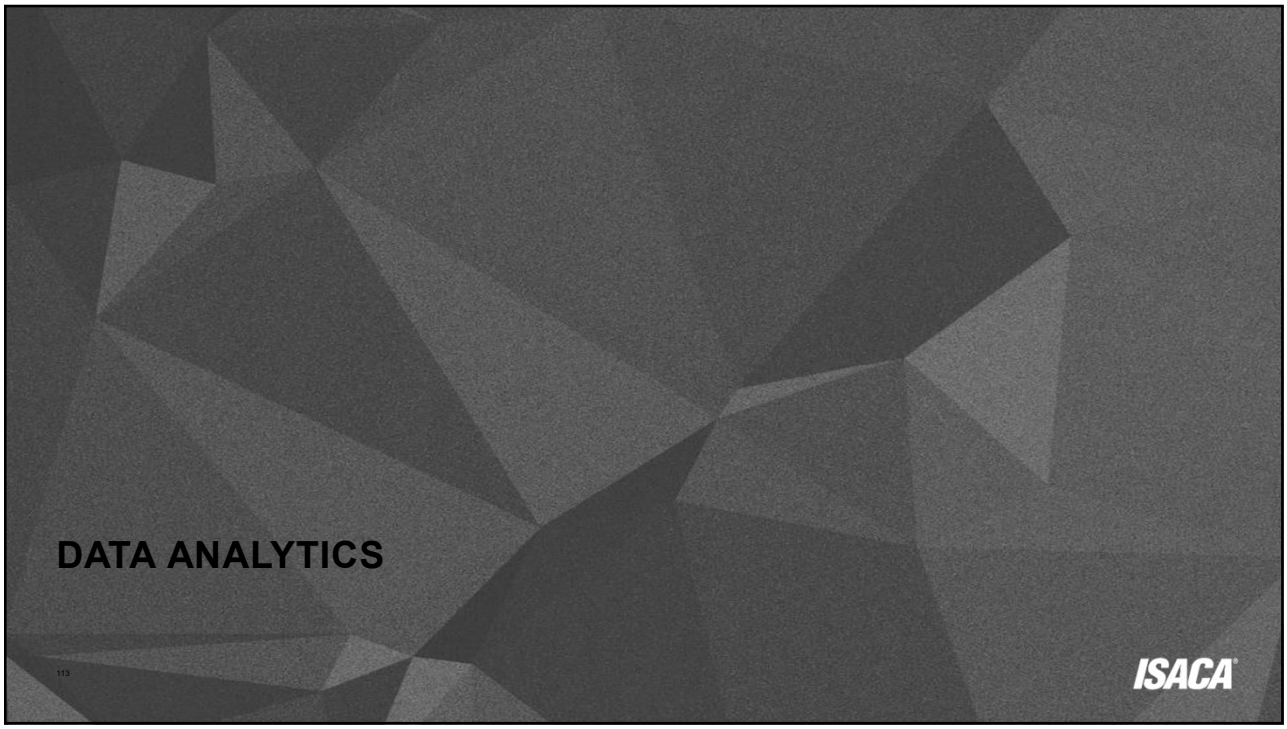
A. Complexity of the organization's operation
B. Findings and issues noted from the prior year
C. Purpose, objective and scope of the audit
D. Auditor's familiarity with the organization



DISCUSSION QUESTION

Which of the following does a lack of adequate controls represent?

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



DATA ANALYTICS

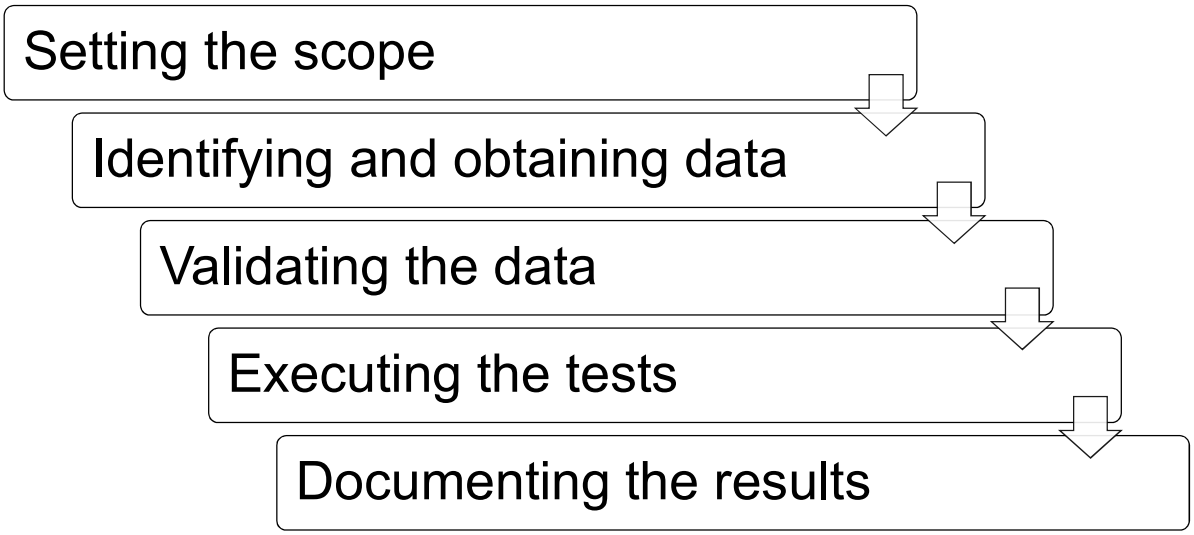
An IS auditor can use data analytics to:

- Determine the operational effectiveness of the current control environment.
- Determine the effectiveness of antifraud procedures and controls.
- Identify business process errors.
- Identify business process improvements and inefficiencies in the control environment.
- Identify exceptions or unusual business rules.
- Identify fraud.
- Identify areas where poor data quality exists.
- Perform risk assessment at the planning phase of an audit.

114

ISACA

COLLECTING DATA



115

ISACA

CAATS TOOLS AND TECHNIQUES

CAATs help IS auditors collect sufficient, relevant and useful evidence that may only exist in electronic form.

They are particularly useful when auditing systems that have different hardware and software environments, data structures, record formats or processing functions.

Tools and Techniques

- Generalized audit software (GAS)
- Utility software
- Debugging and scanning software
- Test data
- Application software tracing and mapping
- Expert systems

ISACA

CAAT CONSIDERATIONS

Before the use of a CAAT, consider:

- Ease of use, both for existing and future audit staff
- Training requirements
- Complexity of coding and maintenance
- Flexibility of uses
- Installation requirements
- Processing efficiencies (especially with a PC CAAT)
- Effort required to bring the source data into the CAATs for analysis
- Ensuring the integrity of imported data by safeguarding their authenticity
- Recording the time stamp of data downloaded at critical processing points to sustain the credibility of the review
- Obtaining permission to install the software on the auditee servers
- Reliability of the software
- Confidentiality of the data being processed

ISACA

AUDIT TOOLS

Figure 1.13—Continuous Audit Tools—Advantages and Disadvantages

	SCARF/EAM	Snapshots	Audit Hooks	ITF	CIS
Complexity	Very high	Medium	Low	High	Medium
Useful when:	Regular processing cannot be interrupted.	An audit trail is required.	Only select transactions or processes need to be examined.	It is not beneficial to use test data.	Transactions meeting certain criteria need to be examined.

118

ISACA

REPORTING AND COMMUNICATION

119

ISACA

COMMUNICATION OF RESULTS

The IS auditor communicates the audit results in an exit interview with management.

During the exit interview, the IS auditor should:

- Ensure that the facts presented in the report are correct.
- Ensure that the recommendations are realistic and cost-effective, and if not, seek alternatives through negotiation with auditee management.
- Recommend implementation dates for agreed upon recommendations.

The IS auditor can present the results of the audit in an executive summary or a visual presentation.

ISACA

COMMUNICATION OF RESULTS (CONT'D)

Before communicating results of the audit to senior management, the IS auditor should discuss the findings with the key process owners to gain an agreement on the findings and develop a course of corrective action.

IS auditors should feel free to communicate issues or concerns with senior management or the audit committee.

AUDIT REPORT OBJECTIVES

- Formally present the audit results to the auditee (and the audit client if different from the auditee).
- Serve as formal closure of the audit engagement.
- Provide statements of assurance and, if needed, identification of areas requiring corrective action and related recommendations.
- Serve as a valued reference for any party researching the auditee or audit topic.
- Serve as the basis for a follow-up audit if audit findings were presented.
- Promote audit credibility when well developed and well written.

ISACA

AUDIT REPORT

Audit reports present the IS auditor's findings and recommendations to management. They are the end product of the IS audit work.

The report should be balanced, describing not only negative issues in terms of findings but positive constructive comments regarding improving processes and controls or effective controls already in place.

ISACA IS Audit and Assurance Standard 1401 Reporting

ISACA

AUDIT REPORT STRUCTURE

The audit report format and structure is dependent on the organization's audit policies and procedures, but reports usually have the following structure and content:

- An introduction to the report, including the audit objectives, limitations and scope, the period of audit coverage, and a general statement on the procedures conducted and processes examined during the audit, followed by a statement on the IS audit methodology and guidelines
- Audit findings, often grouped in sections by materiality and/or intended recipient
- The IS auditor's overall conclusion and opinion on the adequacy of controls and procedures, and the actual potential risk identified as a consequence of detected deficiencies
- The IS auditor's reservations or qualifications with respect to the audit
- Detailed audit findings and recommendations
- A variety of findings, some of which may be quite material while others are minor in nature

ISACA

AUDIT DOCUMENTATION

Audit documentation provides the necessary evidence that support the audit findings and conclusions.

It should be clear, complete, and easily retrievable.

It is the property of the auditing entity and should only be accessible to authorized personnel.

All audit documentation should be:

- Dated
- Initialed
- Page-numbered
- Self-contained
- Properly labeled
- Kept in custody

ISACA IS Audit and Assurance Guideline 2203 Performance and Supervision

ISACA

AUDIT DOCUMENTATION (CONT'D)

Audit documentation should include, at a minimum, a record of the following:

- Planning and preparation of the audit scope and objectives
- Description and/or walk-throughs on the scoped audit area
- Audit program
- Audit steps performed and audit evidence gathered
- Use of services of other auditors and experts
- Audit findings, conclusions and recommendations
- Audit documentation relation with document identification and dates

Documentation must include all information required by laws and regulations, contractual stipulations and professional standards.

ISACA

FOLLOW-UP ACTIVITIES

Auditing is an ongoing process.

It is the IS auditor's responsibility to ensure that management has taken appropriate corrective actions.

A follow-up program should be implemented to manage follow-up activities.

When the follow-up occurs depends on the criticality of the audit findings.

Results of the follow-up should be communicated to the appropriate level of management.

ISACA IS Audit and Assurance Standard 1402 Follow-up Activities

ISACA

ACTIVITY

You have completed testing of the organization's security information and event monitoring system. During this review you have identified several significant findings:

- Threat events are not being detected.
- Validated threat events are not being reported.

What is the **BEST** course of action in communicating these results during testing?

What is the best approach when communicating these findings to the executive team?

DISCUSSION QUESTION

Which of the following is the **PRIMARY** requirement in reporting results of an IS audit? 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.

DISCUSSION QUESTION

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.

ACTIVITY

Through testing, the IS auditor determined that threat events are not being detected and reported. What order would the auditor recommend for management to take corrective action?

- Threat events are not being detected.
- Validated threat events are not being reported.
- Security monitoring is only 40 hours/5 days a week.
- Personnel are not being trained to operate the log monitoring system.

Which of these IS findings' corrective actions needs to be assessed first?

DISCUSSION QUESTION

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.

DISCUSSION QUESTION

The **PRIMARY** objective of performing a post incident review is that it presents an opportunity to:

A. improve internal control procedures.
B. harden the network to industry good practices.
C. highlight the importance of incident response management to management.
D. improve employee awareness of the incident response process.

QUALITY ASSURANCE AND IMPROVEMENT OF THE AUDIT PROCESS

134

ISACA

CONTROL SELF-ASSESSMENT

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. It is not intended to replace audit's responsibilities but to enhance them.

135

ISACA

INTEGRATING AUDITING

The integrated audit process typically involves:

- Identification of risk faced by the organization for the area being audited.
- Identification of relevant key controls.
- Review and understanding of the design of key controls.
- Testing that key controls are supported by the IT system.
- Testing that management controls operate effectively.
- A combined report or opinion on control risk, design and weaknesses.

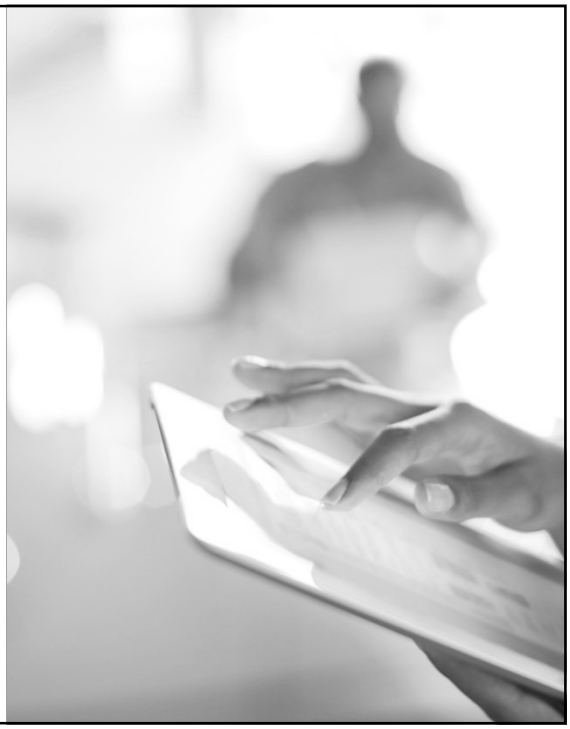
136

ISACA

DISCUSSION QUESTION

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. Review of the audit charter
C. Identification of key information owners
D. Development of a risk assessment



DISCUSSION QUESTION

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 (CAATs)
C. Compliance testing
D. Integrated test facility (ITF)

PRACTICE QUESTIONS

139

ISACA

PRACTICE QUESTION

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.

PRACTICE QUESTION

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

141

PRACTICE QUESTION

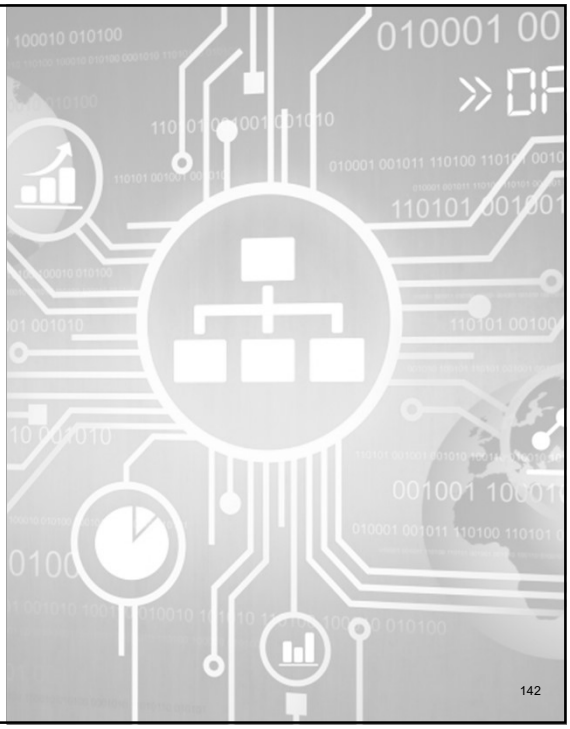
An IS auditor notes that failed login attempts to a core financial system are automatically logged and the logs are retained for a year by the organization. This logging is:

A. An effective preventive control.

B. A valid detective control.

C. Not an adequate control.

D. A corrective control.

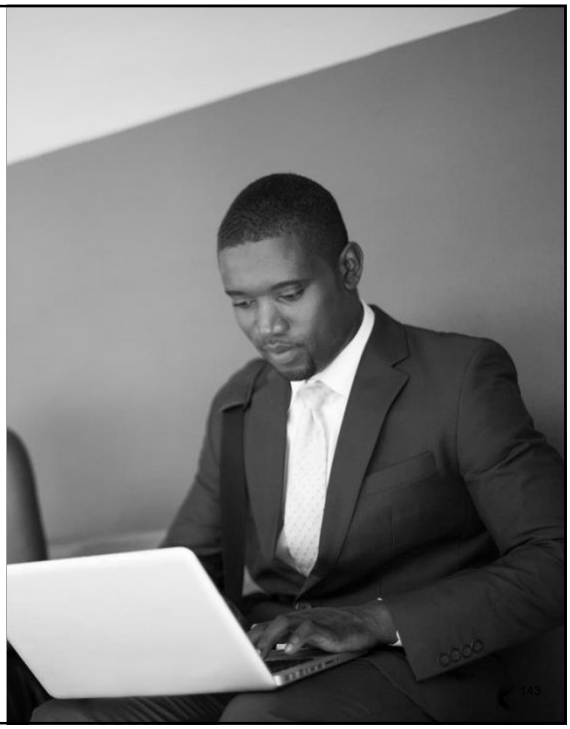


142

PRACTICE QUESTION

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.



PRACTICE QUESTION

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

PRACTICE QUESTION

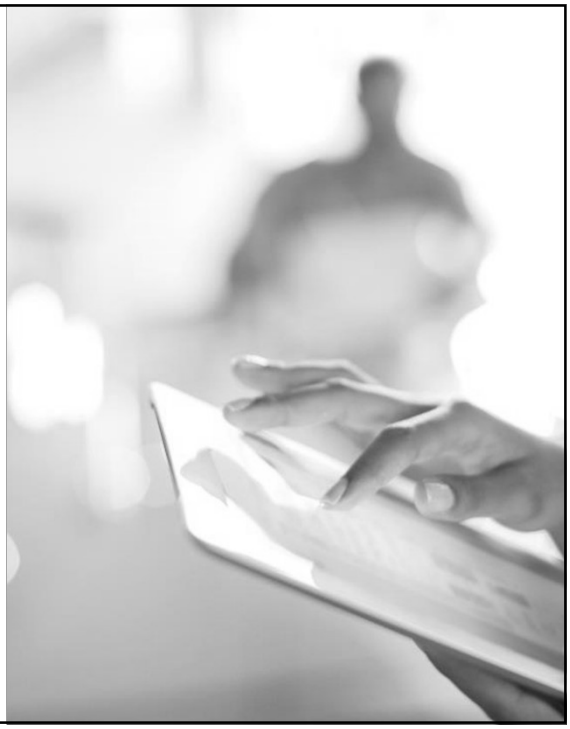
The effect of which of the following should have priority in planning the scope and objectives of an IS audit?

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

PRACTICE QUESTION

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.



PRACTICE QUESTION

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

PRACTICE QUESTION

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

PRACTICE QUESTION

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.

149

PRACTICE QUESTION

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

150

PRACTICE QUESTION

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

DOMAIN 1 REVIEW

As an IS auditor, you should now be able to able to:

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Conduct an audit in accordance with IS audit standards and a risk-based IS audit strategy.
- Communicate audit progress, findings, results, and recommendations to stakeholders.
- Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organization's IT policies and practices.