CISA®

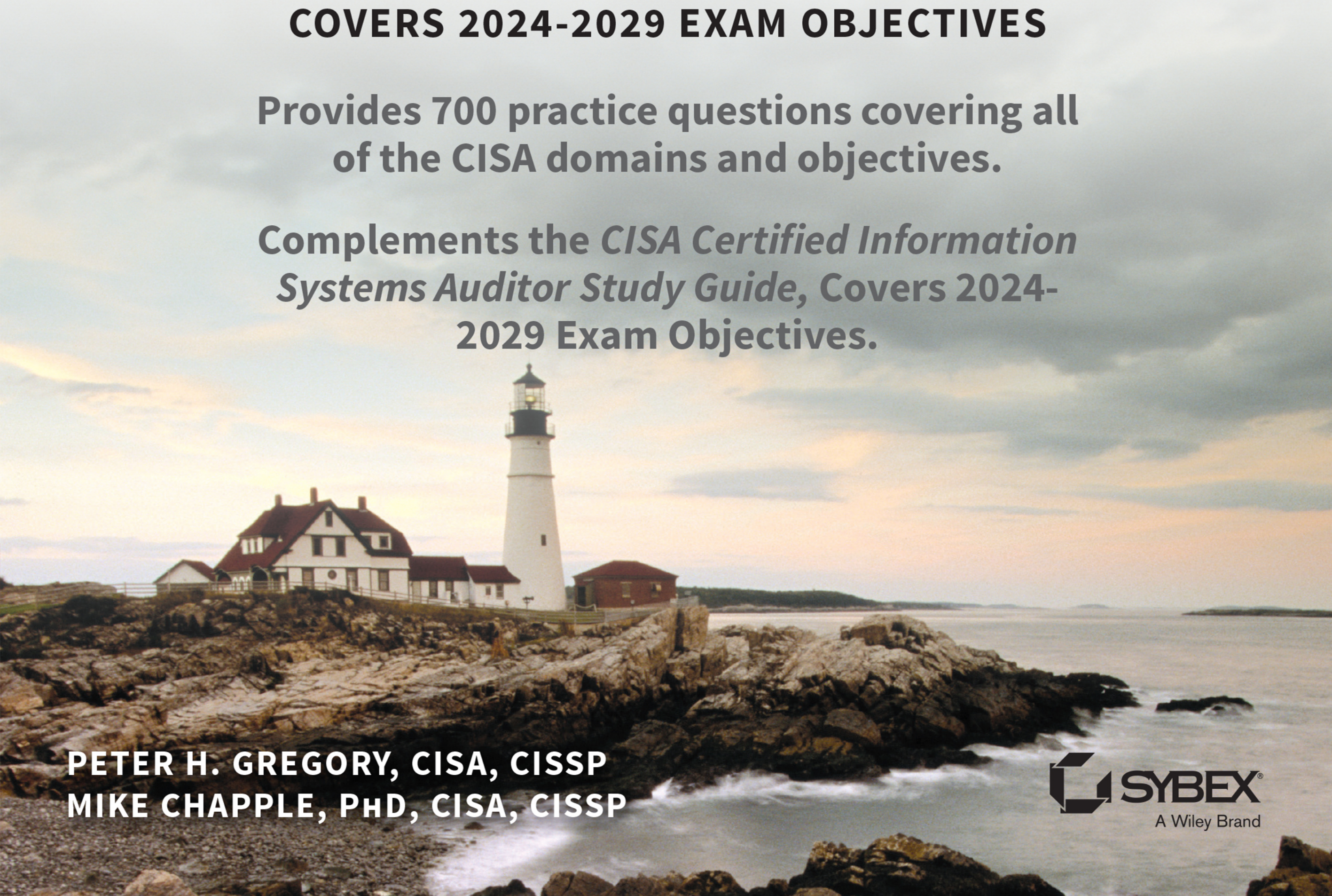
CERTIFIED INFORMATION SYSTEMS AUDITOR

PRACTICE TESTS

COVERS 2024-2029 EXAM OBJECTIVES

Provides 700 practice questions covering all of the CISA domains and objectives.

Complements the *CISA Certified Information Systems Auditor Study Guide*, Covers 2024-2029 Exam Objectives.



PETER H. GREGORY, CISA, CISSP
MIKE CHAPPLE, PHD, CISA, CISSP

SYBEX®
A Wiley Brand

CISA®

Certified Information Systems Auditor Practice Tests

Covers 2024–2029 Exam Objectives

CISA®

Certified Information Systems Auditor Practice Tests

Covers 2024–2029 Exam Objectives

Peter H. Gregory, CISA, CISSP

Mike Chapple, Ph.D., CISA, CISSP

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Limit of Liability/Disclaimer of Warranty: While the publisher and authors have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993. For product technical support, you can find answers to frequently asked questions or reach us via live chat at https://sybexsupport.wiley.com.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our website at www.wiley.com.

Library of Congress Control Number: 2025908051

Print ISBN: 9781394290109
ePdf ISBN: 9781394290123
ePub ISBN: 9781394290116
oBook ISBN: 9781394324460

Cover Design: Wiley
Cover Image: © Jeremy Woodhouse/Getty Images

To my grandchildren – may they grow up in a safer world.
—Peter

To my wife, Renee. We are a quarter century into this adventure together and yet we still find ourselves standing on the precipice of change. Here's to what's next!
—Mike

Acknowledgments

Books like this involve work by many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank our acquisitions editor, Jim Minatel, who jumped through some incredible hoops to make this project possible.

We also greatly appreciated the editing and production team for the book, including Christine O'Connor, the managing editor, who brought years of experience and great talent to the project; Archana Pragash, the project manager, who kept the train on the tracks; Bobby Rogers and Jessica Chang, the technical editors, who provided insightful advice and gave wonderful feedback throughout the book; and Liz Britten, the production editor, who guided us through layouts, formatting, and final cleanup to produce a great book. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who made the book and companion materials into a finished product.

Shahla Pirnia, Elastos Chimwanda, Craig Sheffield, and Laurence Urbano, members of Mike's team at CertMike.com, were instrumental in helping us get all the details straightened out as we prepared the manuscript.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families, who supported us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Peter H. Gregory, CISSP, CISM, CISA, CRISC, CIPM, CDPSE, CCSK, A/CCRF, A/CCRP, A/CRMP, is the author of more than 60 books on security and technology, including *Solaris Security* (Prentice Hall, 2000), *The Art of Writing Technical Books* (Waterside, 2022), *CISA Certified Information Systems Auditor Study Guide* (John Wiley, 2025), *Chromebook For Dummies* (Wiley, 2023), and *Elementary Information Security* (Jones & Bartlett Learning, 2024).

Peter is a career semi-retired technologist and security executive. Earlier, he held security leadership positions at GCI (www.gci.com), Optiv Security (www.optiv.com), and Concur Technologies (www.concur.com). Peter is an advisory board member for the University of Washington and Seattle University for education programs in cybersecurity. He is a 2008 graduate of the FBI Citizens' Academy.

Peter resides in Central Washington State and can be found at www.peterhgregory.com.

Mike Chapple, PhD, CISA, CISSP, CISM, CIPP/US, CIPM, CCSP, CySA+, is the author of more than 50 books, including the best-selling *CISSP ISC2 Certified Information Systems Security Professional Official Study Guide* (Sybex, 2024), the *CISA Certified Information Systems Auditor Study Guide* (John Wiley, 2025), and the *CISSP ISC2 Official Practice Tests* (Sybex 2024). He is a cybersecurity professional with 25 years of experience in higher education, the private sector, and government.

Mike currently serves as teaching professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Mike previously served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. He also spent four years in the information security research group at the National Security Agency and served as an active-duty intelligence officer in the US Air Force.

Mike earned both his BS and PhD degrees in computer science and engineering from Notre Dame. He also holds an MS in computer science from the University of Idaho and an MBA from Auburn University.

Learn more about Mike and his other security certification materials at his website, https://CertMike.com.

About the Technical Editors

Bobby Rogers is a senior cybersecurity professional with more than 30 years in the field. He serves as a cybersecurity auditor and virtual chief information security officer (vCISO) for a variety of clients. He works with a major engineering company in Huntsville, Alabama, helping to secure networks and manage cyber risk for its customers. In addition to numerous educational institutions, Bobby's customers have included the US Army, NASA, the State of Tennessee, and private/commercial companies and organizations. Bobby's specialties are cybersecurity engineering, security compliance, and cyber risk management, but he has worked in almost every area of cybersecurity, including network defense, computer forensics and incident response, and penetration testing.

He has narrated and produced more than 30 computer training videos for several training companies. He is the author of McGraw-Hill Education's *CompTIA CySA+ Cybersecurity Analyst Certification Passport (Exam CS0-002),* 1st Edition and *CISSP Certification Passport,* 1st Edition; coauthor of *Certified in Risk and Information Systems Control (CRISC) All-in-One Certification Guide*, 1st and 2nd editions; and contributing author/technical editor for the popular *CISSP All-in-One Exam Guide* (7th, 8th, and 9th editions).

Jessica Chang is a licensed CPA in the state of Colorado with more than 15 years of public accounting and general accounting experience in multiple leadership roles. She has worked in various industries, including telecommunications, hospitality, real estate, and e-commerce, and has served as the chief audit executive for multiple companies.

Contents at a Glance

Introduction

Congratulations on choosing to become a Certified Information Systems Auditor (CISA). Whether you have worked for several years in information systems auditing or have just recently been introduced to the world of controls, assurance, and security, don't underestimate the hard work and dedication required to obtain and maintain CISA certification. Although ambition and motivation are essential, the rewards of being CISA certified can far exceed the effort.

You probably never imagined yourself working in auditing or looking to obtain a professional auditing certification. Perhaps the increase in legislative or regulatory requirements for information system security led to your introduction to this field. Or, possibly, you noticed that CISA-related career options are increasing exponentially, and you have decided to get ahead of the curve. You aren't alone; since the inception of the CISA certification in 1978, more than 200,000 professionals worldwide reached the same conclusion and have earned this well-respected certification. Welcome to the journey and the amazing opportunities that await you.

How to Use This Book

This book is a companion to the *CISA Certified Information Systems Auditor Study Guide: Covers 2024 Exam Objectives (Sybex, 2025, Gregory/Chapple)*. If you're looking to test your knowledge before you take the CISA exam, this book will help you by providing a combination of 700 questions that cover the CISA domains with easily understood explanations for correct answers.

Since this is a companion to the *CISA Certified Information Systems Auditor Study Guide*, this book is designed to be similar to taking the CISA exam. It contains standard multiple-choice questions similar to those you may encounter in the certification exam itself. The book is divided into five chapters, each corresponding to the five domains in the CISA Job Practice.

We have compiled this information in both books to help you understand the commitment needed, prepare for the exam, and maintain your certification. Not only do we wish you to prepare for and pass the exam with flying colors, but we also provide you with the information and resources to maintain your certification and represent yourself and the professional world of information system (IS) auditing proudly with your new credentials.

If you're preparing for the CISA exam, you'll undoubtedly want to find as much information as possible about information systems and auditing. The more information you have, the better off you'll be when attempting the exam. The companion study guide was written with that in mind. The goal was to provide enough information to prepare you for the test, but not so much that you'll be overloaded with information outside the exam's scope.

Together, these books present the material at an intermediate technical level. Experience with and knowledge of security and auditing concepts will help you fully understand the challenges you'll face as an information systems auditor.

If you can answer 80% or more of the review questions correctly for a given domain, you can feel safe moving on to the next domain. If you're unable to answer that many correctly, reread the companion book chapter and try the questions again. Your score should improve.

Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

About ISACA

ISACA (formerly known as the Information Systems Audit and Control Association) is a recognized leader in control, assurance, and IT governance. Formed in 1967, this nonprofit organization represents more than 180,000 professionals in more than 188 countries. ISACA administers several exam certifications, including:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Certified in Governance of Enterprise IT (CGEIT)
- Certified Cybersecurity Operations Analyst (CCOA)

The certification program has been accredited under ISO/IEC 17024:2012, which means that ISACA's procedures for accreditation meet international requirements for quality, continuous improvement, and accountability.

If you're new to ISACA, we recommend you tour the organization's website (www.isaca.org) and familiarize yourself with the available guides and resources. In addition, if you're near one of the 225 local ISACA chapters in 99 countries worldwide, consider contacting the chapter board for information on local meetings, training days, conferences, or study sessions. You may be able to meet other IS auditors who can give you additional insight into the CISA certification and the audit profession.

Established in 1978, the CISA certification primarily focuses on audit, controls, assurance, and security. It certifies the individual's knowledge of testing and documenting IS controls and their ability to conduct formal IS audits. Organizations seek qualified personnel for assistance with developing and maintaining robust control environments. A CISA-certified individual is a great candidate for these positions.

The CISA Exam

The CISA exam is designed to be a vendor-neutral certification for information systems auditors. ISACA recommends this certification for those who already have experience in auditing and want to demonstrate that experience to current and future employers.

The exam covers five major domains:

1. Information Systems Auditing Process
2. Governance and Management of IT
3. Information Systems Acquisition, Development, and Implementation
4. Information Systems Operations and Business Resilience
5. Protection of Information Assets

These five areas include a range of topics, from enterprise risk management to evaluating cybersecurity controls. They focus heavily on scenario-based learning and the role of the information systems auditor in various scenarios. You'll need to learn a lot of information, but you'll be well rewarded for possessing this credential. ISACA reports that the average salary of CISA credential holders is more than $145,000. And according to *Certification Magazine*'s 2023 salary survey, ISACA credentials, including CISA, are among the top 10 highest paying in IT.

The CISA exam includes only standard multiple-choice questions. Each question has four possible answer choices, and only one of those answers is correct. When taking the test, you'll likely find some questions where you think multiple answers might be correct. In those cases, remember that you're looking for the *best* possible answer to the question!

The exam costs $575 for ISACA members and $760 for non-members. More details about the CISA exam and how to take it can be found at www.isaca.org/credentialing/cisa

You'll have four hours to take the exam and be asked to answer 150 questions during that time. Your exam will be scored on a scale ranging from 200 to 800, with a passing score of 450.

NOTE

ISACA frequently does what is called *item seeding*, which is the practice of including unscored questions on exams. It does so to gather psychometric data, which is then used when developing new versions of the exam. Before you take the exam, you will be told that your exam may include these unscored questions. So, if you come across a question that does not appear to map to any of the exam objectives—or, for that matter, does not appear to belong in the exam—it is likely a seeded question. However, you never really know whether a question is seeded, so always try to answer every question.

Taking the Exam

Once fully prepared to take the exam, you can visit the ISACA website to register. Currently, ISACA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam on your own computer through a remote proctoring service.

In-Person Exams

ISACA partners with PSI Exams testing centers, so your next step will be to locate a testing center near you. In the US, you can do this based on your address or your ZIP code, whereas non-US test takers may find it easier to enter their city and country. You can search for a test center near you on the PSI Exams website: https://www.psiexams.com

Now that you know where you'd like to take the exam, simply set up a PSI testing account and schedule an exam on the site.

On the day of the test, bring a government-issued identification card or passport that contains your full name (exactly matching the name on your exam registration), your signature, and your photograph. Be sure to show up with plenty of time before the exam starts. Remember that you cannot take your notes, electronic devices (including smartphones and watches), or other materials into the testing center with you.

At-Home Exams

ISACA also offers online exam proctoring. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

Due to the rapidly changing nature of the at-home testing experience, candidates wishing to pursue this option should check the ISACA website for the latest details.

One critical fact worth noting is that you must have a computer with a webcam and full administrative control over the computer. You'll likely have some difficulty using an employer-based computer that restricts your control. We recommend that you use a personally owned computer instead.

After the CISA Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam. You're now ready to begin the certification application process, described here.

Meeting the Experience Requirement

The CISA program is designed to demonstrate that an individual is a qualified information systems auditor. That requires more than just passing a test – it also requires real hands-on work experience.

The basic CISA work experience requirement is that you must have five years of work experience in information systems audit, controls, assurance, or security. If your work aligns with any job practice statements found later in this introduction, that experience likely qualifies.

You will be required to get your work experience verified by your supervisor or manager for each organization where you claim experience.

If you're a current information systems auditor or cybersecurity professional, you may find it easy to meet these requirements. If you don't yet meet the experience requirement, you may still take the exam, and then you'll have five years to gain the experience and become fully certified after passing the test.

Some waivers are available that can knock one, two, or three years off your experience requirement:

- If you hold an associate's degree in any field, you qualify for a one-year waiver.
- If you hold a bachelor's, master's, or doctoral degree in any field, you qualify for a two-year waiver.
- If you hold a master's degree in information systems or a related field, you qualify for a three-year waiver.
- If you hold full certification from the Chartered Institute of Management Accountants (CIMA), you qualify for a two-year waiver.
- If you are a member of the Association of Chartered Certified Accountants (ACCA), you qualify for a two-year waiver.

NOTE These waivers may not be combined. You may only use *one* of these waiver options against your certification requirements.

You must have earned all of the experience used toward your requirement within the 10 years preceding your application or within five years of the date you pass the exam.

Once you complete your application, you must acknowledge the ISACA Terms and Conditions Agreement and pay a US $50 application processing fee. When you have received final approval from ISACA, you can include the CISA moniker in your professional matters, including your email signature, resume, social media, and other materials.

Maintaining Your Certification

Information systems auditing is constantly evolving, with new threats and controls arising regularly. All CISA holders must complete continuing professional education annually to keep their knowledge current and their skills sharp. The guidelines around continuing professional education are somewhat complicated, but they boil down to two main requirements:

- You must complete 120 hours of credit every three years to remain certified.
- You must have at least 20 credit hours every year during that cycle.

You must meet both of these requirements. For example, if you earn 120 credit hours during the first year of your certification cycle, you still must earn 20 additional credits in each of the next two years.

Continuing education requirements follow calendar years, and your clock will begin ticking on January 1 of the year after you earn your certification. You are allowed to start earning credits immediately after you're certified. They'll just count for the following year.

There are many acceptable ways to earn CPE credits, many of which do not require travel or attending a training seminar. The important requirement is that you generally do not earn CPEs for work that you perform as part of your regular job. CPEs are intended to cover professional development opportunities outside of your day-to-day work. You can earn CPEs in several ways:

- Attending conferences
- Attending training programs
- Attending professional meetings and activities
- Taking self-study courses
- Participating in vendor marketing presentations
- Teaching, lecturing, or presenting
- Publishing articles, monographs, or books
- Participating in the exam development process
- Volunteering with ISACA
- Earning other professional credentials
- Contributing to the profession
- Mentoring

For more information on the activities that qualify for CPE credits, visit this site: www.isaca.org/credentialing/how-to-earn-cpe.

Additional Study Tools

This book has additional study tools to help you prepare for the exam. They include the following.

NOTE Go to www.wiley.com/go/Sybextestprep to register and gain access to this interactive online learning environment and test bank with study tools.

Sybex Test Preparation Software

Sybex's test preparation software lets you prepare with electronic test versions of the review questions from each chapter, the practice exam, and the bonus exam included in this book. You can build and take tests on specific domains or by chapter, or cover the entire set of CISA exam objectives using randomized tests.

Bonus Practice Exams

In addition to the practice questions for each chapter, this book includes two full 150-question practice exams. We recommend using them both to test your preparedness for the certification exam.

CISA Exam Objectives

ISACA publishes relative weightings for each of the exam's objectives. The following table lists the five CISA domains and the extent to which they are represented on the exam.

Domain	% of Exam
1. Information Systems Auditing Process	18%
2. Governance and Management of IT	18%
3. Information Systems Acquisition, Development, and Implementation	12%
4. Information Systems Operations and Business Resilience	26%
5. Protection of Information Assets	26%

Chapter

1

The Audit Process

THIS CHAPTER COVERS CISA DOMAIN 1, "INFORMATION SYSTEMS AUDITING PROCESS," AND INCLUDES QUESTIONS FROM THE FOLLOWING TOPICS:

- Audit management
- ISACA auditing standards and guidelines
- Audit and risk analysis
- Internal controls
- Performing an audit
- Control self-assessments
- Audit recommendations

The topics in this chapter represent 18% of the CISA examination.

This topic is fully covered in the companion guide, "CISA Certified Information Systems Auditor Study Guide," in Chapter 2.

Questions

You can find the answers to the questions in Appendix A.

1. The IT Assurance Framework consists of all of the following except:
   - **A.** ISACA Code of Professional Ethics
   - **B.** IS audit and assurance standards
   - **C.** ISACA Audit Job Practice
   - **D.** IS audit and assurance guidelines

2. An auditor is examining an IT organization's change control process. The auditor has determined that Change Advisory Board (CAB) meetings take place on Tuesdays and Fridays, where planned changes are discussed and approved. The CAB does not discuss emergency changes that are not approved in advance. What opinion should the auditor reach concerning emergency changes?
   - **A.** The CAB should not be discussing changes made in the past.
   - **B.** The CAB should be discussing recent emergency changes.
   - **C.** Personnel should not be making emergency changes without CAB permission.
   - **D.** Change control is concerned only with planned changes, not emergency changes.

3. A conspicuous video surveillance system would be characterized as what type(s) of control?
   - **A.** Detective and deterrent
   - **B.** Detective only
   - **C.** Deterrent only
   - **D.** Preventive and deterrent

4. Michael is developing an audit plan for an organization's data center operations. Which of the following will help Michael determine which controls require potentially more scrutiny than others?
   - **A.** Security incident log
   - **B.** Last year's data center audit results
   - **C.** Risk assessment of the data center
   - **D.** Data center performance metrics

5. An organization processes payroll and expense reports for thousands of corporate customers in an SAAS-based environment. Those customers want assurance that the organization's processes are effective. What kind of audit should the organization undertake?
   - **A.** Compliance audit
   - **B.** Operational audit
   - **C.** Service provider audit
   - **D.** IS audit

6. An audit project has been taking far too long, and management is beginning to ask questions about its schedule and completion. This audit may be lacking:

   A. Effective project management

   B. Cooperation from individual auditees

   C. Enough skilled auditors

   D. Clearly stated scope and objectives

7. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions. This type of sampling is known as:

   A. Judgmental sampling

   B. Random sampling

   C. Stratified sampling

   D. Statistical sampling

8. An auditor is auditing an organization's user account request and fulfillment process. What is the first type of evidence collection the auditor will likely want to examine?

   A. Observation

   B. Document review

   C. Walkthrough

   D. Corroborative inquiry

9. A lead auditor is building an audit plan for a client's financial accounting system. The plan calls for periodic testing of a large number of transactions throughout the audit project. What is the best approach for accomplishing this?

   A. Reperform randomly selected transactions.

   B. Periodically submit test transactions to the audit client.

   C. Develop one or more CAATs.

   D. Request a list of all transactions to analyze.

10. A lead auditor is building an audit plan for a client's financial transaction processing system. The audit will take approximately three months. Which of the following is the best approach for reporting audit exceptions to the audit client?

    A. Report the exceptions to the audit committee.

    B. List the exceptions in the final audit report.

    C. Include the exceptions in a weekly status report.

    D. Advise the client of exceptions as they are discovered and confirmed.

11. Which of the following is true about the ISACA Audit Standards and Audit Guidelines?
    - **A.** ISACA Audit Standards are mandatory.
    - **B.** ISACA Audit Standards are optional.
    - **C.** ISACA Audit Guidelines are mandatory.
    - **D.** ISACA Audit Standards are only mandatory for SOX audits.

12. An auditor is auditing an organization's identity and access management program. The auditor has found that automated workflows are used to receive and track access requests and approvals. However, the auditor has identified a number of exceptions where subjects were granted access without the necessary requests and approvals. What remedy should the auditor recommend?
    - **A.** Monthly review of access approvers
    - **B.** Annual review of access approvers
    - **C.** Annual user access reviews
    - **D.** Monthly user access reviews

13. Why are preventive controls preferred over detective controls?
    - **A.** Preventive controls are easier to justify and implement than detective controls.
    - **B.** Preventive controls are less expensive to implement than detective controls.
    - **C.** Preventive controls stop unwanted events from occurring, whereas detective controls only record them.
    - **D.** Detective controls stop unwanted events from occurring, whereas preventive controls only record them.

14. For the purposes of audit planning, can an auditor rely on the audit client's risk assessment?
    - **A.** Yes, in all cases.
    - **B.** Yes, if the risk assessment was performed by a qualified external entity.
    - **C.** No. The auditor must perform a risk assessment themselves.
    - **D.** No. The auditor does not require a risk assessment to develop an audit plan.

15. An organization processes payroll and expense reports in an SAAS-based environment for thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?
    - **A.** AUP
    - **B.** PA DSS
    - **C.** PCI DSS
    - **D.** SSAE18

16. An auditor is auditing an organization's system-hardening policy within its vulnerability management process. The auditor has examined the organization's system-hardening standards and wants to examine the configuration of some of the production servers. What is the best method for the auditor to obtain evidence?

A. Capture screenshots from servers selected by the systems engineer during a walkthrough.

B. Request screenshots from servers selected by the systems engineer.

C. Request screenshots of randomly selected servers from the systems engineer.

D. Capture screenshots from randomly selected servers during a walkthrough with the systems engineer.

17. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions, as well as some of the transactions for privileged access requests. This type of sampling is known as:

A. Judgmental sampling

B. Random sampling

C. Stratified sampling

D. Statistical sampling

18. An auditor is auditing an organization's user account request and fulfillment process. The auditor has requested that the control owner describe the process to the auditor. What type of auditing is taking place?

A. Observation

B. Document review

C. Walkthrough

D. Corroborative inquiry

19. An external audit firm is performing an audit of a customer's financial accounting processes and IT systems. While examining a data storage system's user access permissions, the staff auditor discovered the presence of illegal content. What should the staff auditor do next?

A. Notify law enforcement.

B. Inform their supervisor.

C. Notify the auditee.

D. Notify the auditee's audit committee.

20. A QSA auditor in an audit firm has completed a PCI DSS audit of a client and found the client noncompliant with one or more PCI DSS controls. Management in the audit firm has asked the QSA auditor to sign off the audit as compliant, arguing that the client's level of compliance has improved from prior years. What should the QSA auditor do?

A. Refuse to sign the audit report as compliant.

B. Sign the audit report as compliant, under duress.

C. Sign the audit report as compliant.

D. Notify the audit client of the matter.

21. An organization wants to drive accountability for the performance of security controls to their respective control owners. Which activity is the best to undertake to accomplish this objective?

A. Direct control owners to sign a document of accountability.

B. Have the internal audit department audit the controls.

C. Have an external audit firm audit the controls.

D. Undergo control self-assessments (CSAs).

22. An auditor is evaluating a control related to a key card mechanism protecting a data center from unauthorized visitors. The auditor has determined that the key card control is ineffective because visitors often "piggyback" their way into the data center. What detective control should be implemented to compensate for this control deficiency?

A. A video surveillance system with 90-day content retention that records all entrances into and exits from the data center

B. A visitor's log inside the data center that all visitors would be required to sign

C. A man trap

D. A policy requiring all visitors to be escorted

23. A US-based organization processes payroll and expense reports in an SAAS-based environment for thousands of corporate customers. Customers outside the US want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?

A. ISO/IEC 27001

B. SOC2

C. ISAE3402

D. SSAE18

24. A large merchant organization has commissioned a QSA (PCI) audit firm to perform a PCI DSS Report on Compliance (ROC). The audit firm has noted that the merchant's compliance deadline is less than one month away. What should the audit firm do next?

A. File a compliance extension with the PCI Standards Council on behalf of the merchant.

B. Inform the merchant that the ROC can be completed on time.

C. Inform the merchant that the ROC cannot be completed on time and that an extension should be requested.

D. File a compliance extension with the merchant's acquiring bank.

25. An auditor is developing an audit plan for an accounts payable function. Rather than randomly selecting transactions to examine, the auditor wants to select transactions from low, medium, and large payment amounts. Which sample methodology is appropriate for this approach?

A. Judgmental sampling

B. Stratified sampling

C. Nonrandom sampling

D. Statistical sampling

26. A cybersecurity audit firm has completed a penetration test of an organization's web application. The final report contains two findings that indicate the presence of two critical vulnerabilities. The organization disputes the findings because of compensating controls outside the web application interface. How should the audit proceed?

A. The audit firm should remove the findings from the final report.

B. The organization should select another firm to conduct the penetration test.

C. The organization's management should protest the findings and include a letter accompanying the pen test report.

D. The audit firm should permit the customer to include some management comments in the final report.

27. What is the objective of the ISACA audit standard on organizational independence?

A. The auditor's placement in the organization should ensure that the auditor can act independently.

B. The auditor should not work in the same organization as the auditee.

C. To ensure that the auditor has the appearance of independence.

D. To ensure that the auditor has a separate operating budget.

28. An auditor is auditing an organization's risk management process. During the walkthrough, the auditor asked the auditee to list all of the information sources contributing to the process. The auditee cited penetration tests, vendor advisories, nonvendor advisories, and security incidents as inputs. What conclusion should the auditor draw from this?

A. The process is effective because risks are obtained from several disparate sources.

B. The process is ineffective as risk assessments do not occur or contribute to the process.

C. The process is effective because both internal and external sources are used.

D. The process is ineffective because an anonymous tip line was not among the sources.

29. The capability wherein a server is constituted from backup media is known as which type of control?

A. Primary control

B. Manual control

C. Compensating control

D. Recovery control