CISA®: Certified Information Systems Auditor

Study Guide

Fourth Edition

CISA®: Certified Information Systems Auditor

Study Guide

Fourth Edition

David Cannon

with Brian T. O'Hara and Allen Keele

SYBEX®
A Wiley Brand

Development Editor: Kelly Talbot
Technical Editors: Brady Pamplin, Jason James
Production Editor: Rebecca Anderson
Copy Editor: Judy Flynn
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Associate Publisher: Jim Minatel
Media Supervising Producer: Rich Graves
Book Designers: Judy Fung and Bill Gibson
Proofreader: Kim Wimpsett
Indexer: Jack Lewis
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: ©Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-119-05624-9
ISBN: 978-1-119-05625-6 (ebk.)
ISBN: 978-1-119-05640-9 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2015960605

10 9 8 7 6 5 4 3 2 1

About the Author

David L. Cannon, CISA, CCSP, is the founder of CertTest Training Center, a leading CISA training provider. David has more than 20 years' IT training and consulting experience in such industries as IT operations, security, system administration, and management. David teaches CISA preparation courses across the country. He is well respected within the I.S. auditing field and is a frequent speaker and lecturer at the leading security and auditing conferences. David wrote the previous editions of this book, the leading CISA prep guide on the market.

About the Contributors

Brian T. O'Hara, CISA, CISM, CRISC, CISSP, is the Information Security Officer (ISO) for Do it Best Corp. With over 20 years' experience providing security and audit services he has served as the information security officer for Fortune 500 companies and has worked in PCI, healthcare, manufacturing, and financial services providing audit and security advisory services. Prior to entering the field of IS audit, Mr. O'Hara served as program chair for information technology at the largest community college in the country where he helped develop the first NSA Two Year Center of Academic Excellence in Information Security. In addition to contributing to the CISA study guide, he also served as technical editor on the Wiley ISC CISSP and SSCP study guides. He currently serves as the president of the Indiana chapter of ISACA and the Indiana Members Alliance of Infragard, a public-private partnership with the FBI aimed at protecting the nation's critical infrastructures.

Allen Keele is a recognized subject matter expert, consultant, and business systems architect for enterprise risk management (ERM), information security management, governance/risk/compliance (GRC), business continuity management (BCM), fraud control, and purchasing & supply management. He is a 6-time published author, and has achieved over twenty-five professional accreditations including CISA, CISM, CISSP, ISO 31000 CICRA, ISO 27001 CICA, ISO 27001 Lead Auditor, ISO 22301 Certified Business Continuity Manager, and Certified Fraud Examiner. Allen is often featured as a speaker at conferences, expositions, and functions for professional organizations and associations such as the Information Systems Audit and Controls Association (ISACA), the Institute for Internal Auditors (IIA), Ernst & Young, and many others.

Since founding Certified Information Security (`www·certifiedinfosec·com`) in 1999, Allen has led CIS in providing valuable training and consulting services focusing on business strategy, policy, and system development, deployment, and auditing for enterprise risk management, business continuity management, information security management,

fraud control management, and purchasing & supply chain management. His scope of practical expertise includes:

- Leading client organizations' cross-functional committees to develop standards-conforming program architecture and strategy for ERM, GRC, BCM, information security, and fraud control to support organizational objectives, as well as to fulfil industry-specific compliance requirements;
- Enabling clients to establish the necessary strategy, management leadership, policies, and protocols to support organizational certification for ISO 22301 BCM, ISO 27001 Information Security, ISO 9001:2015 Quality Management Systems, and ISO 14001:2015 Environmental Management Systems;
- Delivering critical group executive development sessions to establish requisite specialized management competence throughout the enterprise;
- Leading program project kick-off and deployment;
- Assisting organizations in establishing defined risk context, criteria, and scoping necessary for operational risk assessments and business impact assessments;
- Assisting organizations in developing a formal risk assessment and risk treatment methodology; and
- Leading risk owners and auditors to perform operational risk assessments, information security assessments, fraud risk assessments, and business continuity planning assessments.

Allen Keele can be contacted at CIS headquarters at +1 (904) 406-4311, or at `allenkeele@certifiedinfosec·com`.

About the Technical Editor

Brady Pamplin, CISSP, spent 28 years at Control Data Corporation in many roles, including programmer, instructor, analyst in charge, and project manager. During two years at CertTest Training Center, Brady taught a number of CISSP preparation courses and co-authored the first edition of *CISA Certified Information Systems Auditor Study Guide*. He also was the technical editor of the three subsequent editions. Brady has also worked in telecom companies as a system and network administrator. In 2011, he retired from Alcatel-Lucent as a network architect.

Contents at a Glance

Contents

Introduction

This book is designed for anyone interested in straightforward, honest guidance on passing the Certified Information Systems Auditor (CISA) exam. The CISA certification is one of the hottest entry-level auditor credentials on the market.

It is a trend worldwide for various organizations to upgrade security and prove the existence of strong internal controls. You may have heard of a few of these:

- International Basel III accord for risk management in banking.
- COSO, which includes several variations by country. The US version deals with Sarbanes-Oxley Act (SOX) for public corporations with equivalent controls offered in other stock exchanges worldwide.
- Safe Harbor International Information Privacy Protection.
- US Federal Information Security Management Act (FISMA).
- Payment Card Industry (PCI) standards for credit card processing.
- Health Insurance Portability and Accountability Act (HIPAA).

These are just a few of more than 30 high-profile regulations that demand audited proof of internal controls. Frankly, they present many opportunities for a CISA. This may be the opportunity that you have been looking for, especially if you come from a background of finance or technology.

One of the biggest problems facing regulatory compliance reporting is individuals running testing applications without understanding all the other simultaneous objectives still required. Running software will never make a person a competent auditor. Far too many dependencies exist outside of the testing application. To address this problem, the skeptical auditor mentality is coupled with disciplined written procedures, testing plans, factual reporting of failures even if they are fixed, and objective independence in scope and decisions, which are far more important than automated test results alone.

What Is the CISA Certification?

ISACA offers one of the most recognized certifications in the world for IS auditing: the Certified Information Systems Auditor (CISA) certification. It is recognized worldwide due to excellent marketing. ISACA has active members in more than 180 countries and is recognized as one of the providers in IT governance theory, control theory, and assorted assurance guidelines. ISACA started in 1969 as the Electronic Data Processing Auditors Association, with an objective to develop specific international IS auditing and control standards. Most of the content is bullet points derived from the worldwide financial controls issued by Committee of Sponsoring Organizations of the Treadway Commission (COSO). As a result, ISACA's excellent marketing machine has created a well-known information systems audit certification, the CISA.

ISACA controls the CISA exam worldwide. It is one of the most common credentials in IT governance and IT consulting. CISA, like other ISACA certifications, is easy to obtain because you will never have to perform a single audit procedure to get certified. Another well-known credential you will encounter is the broader and deeper Certified Internal Auditor by Institute of Internal Auditors (IIA).

What Is the Market Potential for Certified IS Auditors?

The CISA world is still moving forward, but the skills gap is rapidly growing wider. After the worldwide banking collapse of 2008, corporations are hiring and retaining consultants in an effort to prove compliance before they get caught short. Consulting companies prefer to contract CISA-certified professionals to help service clients. Large and small organizations are finding themselves at a competitive disadvantage if they're unable to demonstrate a stronger level of internal controls. The myth that an organization can be "too big to fail" has been proven to be false. I'll show you examples as evidence of this in Chapter 1, "Secrets of a Successful Auditor."

One of the fundamental rules of auditing is that participating in the remediation (fixing) of problems found during the audit will compromise the auditor's independence and objectivity. The independent auditor must remain independent or at least objective to certify the results as valid. A second, unrelated auditor should assist in the performance of remediation work. The requirements for regulatory compliance are ongoing, and that means remediation at some level will be ongoing too. In other words, the auditor requirement is actually doubled. The requirements have dramatically increased for clients to keep up.

For over 100 years, organizations have undergone the scrutiny of financial audits. As financial systems have become more and more complex, computer automation has introduced new concerns over the integrity of electronic financial records. In the past, an organization would simply hire a certified public accountant to review its financial records and attest to their integrity. Larger organizations hire certified internal auditors to assist with reviewing internal controls of the business to help reduce the ongoing cost of external audits. Now, the long list of regulations requiring internal controls has focused attention on the information systems. Computers are now the house in which the financial records reside. When verified, tested, fully functional security controls are proven to exist, the executives and personnel can be held responsible for tampering or misrepresentation in electronic records. If you can't prove integrity of the computer environment, you can't trust the integrity of electronic records either.

Why You Should Become a CISA

The majority of uncertified auditors are no more than well-meaning individuals who habitually violate the official audit standards. Here is a short list of the benefits associated with becoming a CISA:

Demonstrates Proof of Professional Achievement The CISA certification provides evidence that you understand basic audit theory enough to pass the written certification

exam. The exam tests your knowledge of auditing concepts and vocabulary related to information systems. Your CISA certification shows that you understand the fundamentals of applying audit concepts to the abstract world of information systems.

Provides Added Value to Your Employer Today's employers are savvy about the value of certification. Your CISA study is expected to illuminate new methods to improve your performance on the job. It's fairly common for individuals to start their auditing career by mimicking a more senior person performing a similar job (as the saying goes, "Monkey see, monkey do"). The goal is to shine the light on specific practices that you should have been following, even if you never heard of them before. Your job performance will improve after you learn the proper foundation to better understand the concepts. After passing the CISA exam, you can take additional hands-on training to perform each audit procedure yourself.

Provides a Basic Credential for Audit Team Members CISA is the minimum credential for members performing audit functions on the audit team. Audit clients are a demanding breed of individuals. The fate of the client's organization may rest on the findings detailed in the auditor's report. There is little room for mistakes. The CISA credential indicates that you are a person who understands enough theory regarding what it will take to deliver trustworthy accurate results. Some auditees will try to mislead you into passing what should be reported as failing. The person reading the audit report needs to understand that your work is accurate. Clients will direct capital and resources to be expended according to the report you provide. The CISA certification helps demonstrate that you are not a biased technician pretending to be an auditor.

Increases Your Market Value The CISA credential is regarded as the entry-level starting point for professional technology auditors. There is no better way to attract the favorable attention of management. It does not matter whether you're internal or external to the organization. Government regulations with more-intrusive requirements are becoming a growing concern for executives. Customers may not understand all the details necessary to describe the job of an auditor; however, your client will recognize that even though you probably don't know the actual audit procedures yet, you are able to talk intelligently about objectives. In addition, audit firms can bill more money for certified professionals.

Provides a Greater Opportunity for Advancement Every organization strives for good people who are self-motivated. What does the lack of certification say about someone? Are they unmotivated? Are they possibly not capable? Or are they simply afraid to try? No manager in their right mind would promote an individual who has not proven their value. Taking the time to get educated shows the world that you are motivated. Getting certified proves you are somebody who wants to get things done. Instead of using words to describe your ability, your CISA credential indicates that you are serious about your job, and people will treat you accordingly.

Builds Your Confidence to Learn Audit Procedures The world today is extremely specialized. Consider that many things of premium value in today's world are certified. We have certified used cars, certified mail, certified public accountants, certified welders,

certified travel agents, certified lawyers, and even certified sandwich artists. Frankly, trade industries perform at least 20 times better at teaching actual procedures and techniques than CISA. It's much harder to be a hair stylist or food service manager because those require months of full performance practicing all the tasks start to finish before achieving certification. Fortunately, CISA training only answers the "why" theory questions; you go elsewhere for training to learn "how" to perform specific audits. The CISA is your first step toward the widespread white-collar office credibility that you desire.

Who Should Buy This Book

If you're serious about becoming a professional technology auditor, this is the book to study. If you're curious about becoming a CISA auditor or lowering the cost of compliance, in this book you will learn how good auditors operate.

The people entering the technology audit field are usually one of the following:

- Finance professionals looking for upward mobility with more interesting challenges
- Industrial control professionals seeking to improve their understanding to gain recognition and advancement
- IT professionals with a desire to leave operations and expand into the lucrative world of consulting or pen testing
- Internal auditors seeking to demystify the control issues within IT (because from news stories, we all know that too many auditors are not properly testing the control elements)

This book is unique in the field of IS auditing. You will benefit by learning the workflow and decision points necessary to be a successful auditor. The chapters take you step-by-step toward obtaining your goal. Inside this book are important details about how to accomplish your job, the exam objectives (listed at the beginning of each chapter), and all of the most important auditing concepts.

Why This Book Is Your Best Choice

This book is specifically designed to help you become a well-respected CISA. There are no jumbled brain dumps or answer cramming exercises here. CertTest has been teaching very successful CISA seminars with hands-on procedural training for several years with outstanding results. This book will never replace our live "See-Do-Run" seminar on how to perform the procedures, but it will help you pass the CISA written exam. The exam alone is just a small stepping-stone in your professional life. Passing the exam does not prove you will be a good auditor. It simply gives your client a reason to listen to you for another 15 seconds. Now you have 15 seconds to demonstrate that you know what you are talking about.

Imagine telling someone that you are a certified juggler of flaming swords. You can bet their next comment would be, "Awesome. Light up the swords and start juggling." Clients are impressed when you show them your skills by performing the tasks, not by you passing

an exam. The goal of this book is to take you through the CISA material better than anyone else by showing you the "how and why" of performing IS audits:

- If you are familiar with technology, this book will help you understand how the auditor must act to be successful. IT professionals often make lousy auditors because auditing is about first understanding the business details. Technology is a secondary tool to accomplish the business goals. Success is achieving the business financial goals with reasonable compliance. Simply focus on how an auditor works instead of thinking like a support technician. Auditors are not techs.
- If you come from a finance background, I'm going to take you through an introductory tour of technology. The CISA is *not* a technician's test. The explanations in this book are technically correct and designed to be simple to understand.

Many opinions exist about how the information systems audit should be performed. This book covers a combination of the official auditing standards of COSO regulations, ISO standards, and ISACA standards. Understanding these standards is necessary for you to be successful. Rest assured that they are not usually in conflict with each other. If in doubt, you should always give priority to the regulations and ISO standards. You'll find that this book contains the valuable information necessary to operate an internal audit or a successful consulting practice. Initially the focus is on helping you pass your exam. However, you will discover that this information can help you earn a great deal more than a paper certificate if you apply it.

Each chapter in this book has been arranged in a logical sequence focusing on a practical application. ISACA produces useful materials written by committees of authors, each contributing a handful of their own pages. I have chosen to take a different route. The material in this book is written in a sequence based upon what CertTest uses to educate its own staff and clients prior to an audit engagement.

You'll start with gaining a firm understanding of the basics and build your way up to the advanced material with almost no duplication. It is strongly suggested that you read the chapters in order, without skipping ahead, because the material in each chapter is important to understanding the material in subsequent chapters. Therefore, focusing on specific chapters out of order may cause problems because the chapters *are not* freestanding units of knowledge.

How to Become a CISA

The CISA designation is provided to individuals who have demonstrated their ability to fulfill the following five requirements based upon the ISO minimum standard for certification of persons:

Pass the CISA Exam The CISA examination is offered three times a year, in June, in September, and again in December. You have to register for the test three months in advance. You can register online at `www.isaca.org` or by mail. The examination is administered by pencil and paper in front of a live test proctor. It consists of 200 multiple-choice questions, and there is a 4-hour time limit. You can expect only a few exam takers

to finish before the "10 minutes left" time warning announcement. A grade above 450 points is required to pass the CISA examination, and you must be in the top one-third of ISACA's grading curve.

Professional Experience in Information Systems Auditing, Control, or Security Because CISA does not check or test anyone's ability to perform a task, the fallback is that you must have five years of IS auditing experience to prove you have enough of a basic entry-level understanding to be a member of an audit team. ISACA will accept up to two years of substitution toward the work experience requirement, as follows:

Related Experience Substitution You can substitute a maximum of one year of financial or operational auditing or information systems experience.

College Credit Hour Substitution The equivalent of an associate or bachelor's degree can be substituted for one or two years, respectively (60 hours or 120 hours).

University Instructor Experience Substitution A full-time university instructor can substitute two years of on-the-job experience toward one year of the IS auditing control or information security experience.

Your CISA test results are valid for five years from the examination date. Even without any related work experience today, you can take the CISA examination to prove you passed the written orientation requirements of basic theory to be on the audit team. While on the team, you can build valuable experience. Certification will be awarded only after you have provided verification of desired work experience (of five years or the equivalent). ISACA limits acceptable experience to that which has occurred within 10 years prior to your application date.

Continuous Adherence to ISACA's Code of Professional Ethics Trust and integrity are paramount to the auditor's profession. You will be required to pledge your ongoing support for adherence to the IS auditor's code of professional ethics.

Adherence to Well-Established IS Auditing Standards The purpose of auditing standards is to ensure quality and consistency. Auditors who fail to meet these standards place clients, themselves, and the profession in peril. ISACA provides information to guide auditors through their professional responsibilities. The auditing standards are based on well-recognized professional practices applied worldwide.

Participate in Continuing Education for Audit Task Proficiency Training and Updates This starts immediately after passing your written exam. You will need more education immediately to learn how to perform individual audit procedure tasks, to learn to operate the different analysis software (like SCAP), and to perform detailed test procedures and many other required tasks that are not covered in the material you will study for the CISA exam. It's always easier to learn by running the procedures than it is by just reading and listening to lectures.

The auditor's job is to apply each of the official industry standards while providing excellent notes so others can independently reproduce the same results. Good work is proven when evidence testing is verified through matching identical results from other

auditors. Poor notes and lack of practice following highly detailed written procedures with limited task proficiency indicate a terrible auditor. Continuous task performance training makes a great auditor.

How to Use This Book and Website

This book is organized into eight chapters. Each begins with a list of chapter objectives that relate directly to the CISA exam.

An "Exam Essentials" section appears near the end of every chapter to highlight a selection of topics that you're likely to encounter during your exam. The exam essentials are intended to guide your study rather than provide a laundry list of details. The goal is to help you focus on the higher-level objectives from each chapter as you move into the next chapter.

At the end of every chapter are basic review questions with explanations. You can use them to help gauge your level of understanding and better focus your study effort. As you finish each chapter, you should review the questions and check whether your answers are correct. If they're not, you should read the relevant section again. Look up any incorrect answers and determine why you missed the question. It may be a case of failing to read the question and properly considering each of the possible answers. It could also be that you did not understand the information. Either way, going through the chapter a second time would be valuable.

We have included several testing features in the book and on the companion website. Following this introduction is an assessment test that will help you gauge your study requirements. Take this test before you start reading the book. It will help you identify areas that are critical to your success. The answers to the assessment test appear after the last question. Each answer includes a short explanation with information directing you to the appropriate chapter for more information.

Included on this book's online-learning environment website at `sybextestbanks.wiley.com` are two practice exams of 200 questions each. In addition, there are more than 300 flashcards. You should use this study guide in combination with your other materials to prepare for the exam.

Take these practice exams as if you were taking the real exam. Just sit down and start each exam without using any reference material. I suggest that you study the material in this book in conjunction with the related ISACA material on IS auditing standards. The official CISA exam is challenging because of the time limit. Most individuals will barely finish the exam before time runs out. Fortunately for you, CertTest's students have a high success rate. You have it within you to become the next certified CISA.

You are ready for your CISA exam when you score higher than 90 percent on the practice examinations and chapter review questions.

The practice exams included on the website are timed to match the pace of your actual CISA exam.

What's Included with the Book

This book includes many helpful items intended to prepare you for the Certified Information Systems Auditor (CISA) exam.

Assessment Test The assessment test at the conclusion of the book's introduction can be used to evaluate quickly where you are with regard to your fundamental understanding of IS audit and audit concepts. This test should be taken prior to beginning your work in this book, and it should help you identify areas in which you are either strong or weak. Note that these questions are purposely more simple than the types of questions you may see on the exams.

Objective Map and Opening List of Objectives At the start of this book is a detailed exam objective map showing you where each of the exam objectives is covered in this book. In addition, each chapter opens with a list of the exam objectives it covers.

Exam Essentials Each chapter ends with a brief overview of the concepts covered in the chapter. I recommend reading through these sections carefully to check your recollection of each topic and returning to any sections of the chapter you're not confident about having mastered.

Chapter Review Questions Each chapter includes review questions. The material for these questions is pulled directly from information that was provided in the chapter. The questions are based on the exam objectives, and they are similar in difficulty to items you might actually receive on the CISA exam.

Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies *CISA: Certified Information Systems Auditor Study Guide, Fourth Edition*, provides a test bank with study tools to help you prepare for the certification exam—and increase your chances of passing it the first time! The test bank includes the following:

Sample Tests All of the questions in this book are provided: the assessment test, which you'll find at the end of this introduction, and the chapter tests that include the review questions at the end of each chapter. In addition, there are two practice exams. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices. New for this edition, more than half of the expanded practice exam questions come from contributor Allen Keele and his industry leading *Allen Keele's 2016 CISA SuperReview.*

Flashcards Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Other Study Tools A glossary of key terms from this book is available as a fully searchable PDF.

Go to `http://sybextestbanks.wiley.com` to register and gain access to this interactive online learning environment and test bank with study tools. Once you register you'll also get access to a limited-time promotion for a discount only available to purchasers of this book on *Allen Keele's 2016 CISA SuperReview.*

How to Use This Book

If you want a solid foundation for preparing for the CISA exam, then look no further. I've spent a lot of time putting together this book with the sole intention of helping you to pass the exam!

This book is loaded with valuable information. You'll get the most out of your study time if you follow this approach:

1. Take the assessment test immediately following this introduction. (The answers are at the end of the test, but no peeking!) It's okay if you don't know any of the answers—that's what this book is for. Carefully read over the explanations for any question you get wrong, and make note of the chapters where that material is covered.
2. Study each chapter carefully, making sure you fully understand the information and the exam objectives listed at the beginning of each one. Again, pay extra-close attention to any chapter that includes material covered in questions you missed on the assessment test.
3. Answer all the review questions at the end of each chapter. Specifically note any questions that confuse you, and study the corresponding sections of the chapter again. And don't just skim these questions—make sure you understand each answer completely.
4. Test yourself using all the electronic flashcards. This is a brand-new and updated flashcard program to help you prepare for the latest CISA exam, and it is a really great study tool.

Learning every bit of the material in this book is going to require applying yourself with a good measure of discipline. So try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. If you work hard, you will be surprised at how quickly you learn this material. If you follow the steps listed here and study with the review questions, practice exams, and electronic flashcards, you will increase your chances of passing the exam.

What to Expect on the CISA Exam

Certainly you are curious about the types of questions you will encounter on the exam. ISACA is very protective of the actual test questions. Let's look at how the test is designed:

- The CISA exam is *not* an IT security test. Candidates will be expected to understand the basic concepts and terminology of what they will be auditing. However, IT security knowledge alone will not help candidates pass the test.
- The CISA exam is *not* a financial auditor exam. Candidates are not expected to be accounting technicians or to perform complex financial transactions.
- The CISA exam is *not* a computer technician exam. Candidates are not expected to build computers or to configure network devices. They are expected to understand the common terminology.
- The entire focus is on how to apply the structured rules of financial auditing to the abstract world of managing information technology.

By properly studying this book, you will better understand the hows and whys of being a successful CISA. Just remember, the IS auditor is a specially trained observer and investigator. We don't actually fix problems; we report findings after using a structured process of investigation. Understanding how to get the right evidence is the key.

How to Fail Your CISA Exam

The CISA exam is based on ISACA's auditing standards and the application of the Statements on Auditing Standards (SAS). Abstract concepts of IT require the auditor to use a different approach to auditing. Adults learn by direct experience or by speaking with other people. Here are the two ways to fail your exam:

Rehearsing Practice Questions More Than Twice One super-bad habit is to rehearse by using practice questions. Studies have proven that the brain stops learning after the second pass over the same question and then it starts memorizing the wording. This causes the brain to record the answer as rote memory rather than to learn the information. As a result, you will likely miss the correct answer on your exam because of the different styles ISACA uses to present the question and the answer choices.

Another big problem is using questions from the Internet that cannot be traced to an official reference source. Bad questions still make the seller money while programming you with the wrong information. Beware of ghostly sellers hiding behind websites without full contact information prominently displayed. I suggest you stick to the questions provided with this book or the CertTest website or buy the ISACA official practice questions. Stop rehearsing the same question after two passes. Instead, reread the corresponding section in the book.

Improper Study Preparation The CISA exam is designed to prevent cram study. You will discover that the structure of the exam questions is rather convoluted. Some of the answer choices will barely fit the question. Just select the best choice that honors the spirit and intent of the audit objectives. It's possible that the best answer is only 51 percent correct. Go with the 51 percent answer if that is the best choice available. This confusion is intentional, to prevent the test taker from using rote memory. The best study technique is to read about 1 hour per night while taking manual notes. Be sure to read all the sections—every page in the order presented. Previous CISA candidates were quite perturbed to discover that the area they assumed to be their strongest was instead where they scored poorly. You may have many years of experience in the subject, but what matters is that your view agrees with ISACA's exam. I have not heard of a single person getting a better score after protesting an official exam question. ISACA uses a professional testing company to run its exam. Protest a question if you must, but I'll wager that you lose the protest and your protest fee in the end.

The Best Way to Pass Your CISA Exam

Be prepared to answer questions about what the *auditor* should be doing. Correct answers are not focused on technical details, as you might expect from an IT equipment support

person. An auditor is an executive position. Senior auditors can meet with the audit committee, composed of the board of directors, each quarter to candidly discuss issues without other executives present. Auditors hire, manage, and directly supervise technical experts using the work of others (audit standards: using the work of others). COSO, ISO, and ISACA standards specifically state that the technical expert is not qualified to provide auditor duties on the audit team.

Always remember, the exam is all about how to implement ISACA audit standards. Relying on what you do at work or practicing rote memory is an excellent path to failure. The purpose of a standard is to represent a uniform unit of measure. Auditors are expected to help executives understand how controls in specific standards function at various levels. Compensating controls use an alternative method that attempts to create the same equivalent effect when other controls are not practical or possible. Because life requires risk-versus-reward decisions, we know everyone will have to compromise and live with some risk present. Hopefully, their preferences are not based on stupid decisions. As auditors, we look at the risks and then decide whether the controls are effective through testing and analysis. We get paid to observe, analyze, and decide. Think about how CSI detectives work on the TV show and you are on the right track. This is the focus of your exam. We listen to evidence via test results. Without enough solid evidence and proper testing, we might issue a qualified opinion, which means we are limiting how the client will use our report.

Never forget that an audit is simply a review of history. Audit opinions are actually scores based on starting with specific audit objectives, collecting enough evidence samples, testing, analyzing results, and reporting. The auditee is the target subject who starts with a score of zero and builds points based on supporting evidence. As auditors, we are expected to use accredited audit procedures. The standards say that auditors simply test the evidence to determine whether a management claim of compliance is supported (possibly true) or unsupported (false). COSO, ISACA, and ISO standards say auditors are *not* responsible for detecting all the problems, nor are we responsible for subsequent acts. If another auditor comes up with different results, it's due to procedural problems, evidence issues, or the weak skills of one of the auditors.

Test Taking and Preparation

The CISA examination is quite difficult unless you are prepared. Preparation requires good study habits and a well-planned schedule of 55 to 65 total hours. You should read or review your notes at least 30 minutes per night, but never more than 2 hours per day. As mentioned, cramming for this examination will not work. If you do pass by cramming, you will probably fail on the job performance, big time.

Let's discuss preparations leading up to test day—specifically, the best method to arrange your schedule for that ace grade.

Thirty-Day Countdown

Review each chapter in your study guide. Remember, this book was written to build your understanding successively with a minimum of duplication. Each chapter elaborates on

information in the preceding chapter. Give extra attention to the subjects that you may have skimmed over earlier. The test is written from the viewpoint of an auditor, using directives from ISACA's world.

Number-one hint: Make sure you are reading from the auditor's perspective.

You should review the electronic flashcards on the accompanying website. It is also an excellent technique to make your own flashcards by using 3″ × 5″ index cards. Take a dozen or two dozen to the office each day for random practice between meetings.

Be sure to run through the practice exams on the website. They are less difficult than the real test but still a good resource to see where you stand. The value of these tests is in improving your resilience and accuracy.

Be sure to request a day of rest. Ask your boss for personal time. Use vacation time if necessary. Most employers will understand after you remind them of the limited testing dates.

Ten-Day Countdown

The exam location may be in a hotel, college, or convention center. It will save you a great deal of time and stress to drive over to visit the test site. You should do this even if you have been there recently. The room number for your test will be printed on your exam acceptance letter. Make it a point to locate the meeting room and physically walk up to touch the door. In colleges, it is possible that room 300 is a significant walk away from room 302. Arriving at the wrong building can ruin your day if it makes you late to the exam.

Convention centers are worse. Unknown to you, there may be a big trade convention or street marathon over the same weekend. Such an event will change the availability of parking in the area. It will also affect the long route you may have to walk in order to enter the examination room.

The best suggestion is to scout the area for a nearby place to eat breakfast. Plan to eat healthily before the exam begins.

Be extra early since the text proctor may have to call ISACA to verify any registration not on the sign-in sheet before letting you in the room. Even though I had my authorization letter in hand, my name did not appear on the registered attendee list, so the exam almost started without me. If the exam starts without you, it's a long wait until the next exam. Over a decade ago my registration was not verified in time, so I got rescheduled to the next year. BE EARLY. It took 26 minutes to verify when I retook the exam to certify again in 2014. As I finally walked in, the exam announcements started before I even got seated. I almost missed it. And yes, I passed the CISA again.

Three-Day Countdown

The best aid to a high score is to take off early on Friday. Remember, the exam is early on Saturday morning. Make a pact with your friends and family to leave you alone all

day Friday. You may consider limiting your diet to simple foods, avoiding anything that is different from usual. This is not the time to experiment.

Also make a pact with yourself: There are no errands or chores more important than passing the exam.

Go to bed earlier than usual. Do whatever it takes. You will need to be up and totally focused by 6 a.m. and out the door early as possible. Try to go to bed by 10 p.m. Set two alarm clocks to get up on time. Put your favorite study materials together in a carrying bag. You will take them with you to the exam for a final glance before being seated for the test. The exam is a "closed book" test.

Do not attempt to cram on Friday night; it will work against you in a long test like the CISA. Just review your notes again. Be sure to run through the flashcards and chapter review questions.

I suggest people with a technical background review Chapter 2, "Governance," and Chapter 3, "Audit Process," twice. If you have a financial background, the best advice is to reread Chapter 4, "Networking Technology Basics," and Chapter 7, "Protecting Information Assets." Practicing drawing the diagrams and models on a separate sheet of paper will help you understand the specific wording of questions and make it easier to select the correct answer. Be prepared to redraw the models from memory during your exam.

Dress for Comfort

This is not a fashion show. It's a long exam, and you need to plan for comfort. Regardless of the season, the testing room is usually one of two extremes: either hot and stuffy or cold and breezy. It does not matter whether the problem is caused by an Arctic snowstorm, overactive heating system, or super strong air conditioner blowing icy snow in your face. You should dress in layers of clothing so you can add a sweater or strip down to a T-shirt for comfort. I took my CISA exam during a Texas summer and froze my buns under the icy blast of the university's air conditioner. I went back to the same room a few years later for my CISM exam and the room was sweltering hot. It's better to dress prepared for anything.

Test Morning

It is time to get up and get moving. Be sure to arrive at the exam early. Test room locations have been known to change overnight, especially at college locations.

After you arrive, you can sit in the hallway while you wait. This is an excellent time to make a final review of your notes. There is no advantage to being seated before 7:30 a.m. Just park yourself within a few feet of the door to ensure that you are not forgotten or missed. You can expect a long line at some test locations. Major cities may have 200 to 300 people sitting in different rooms.

Upon entering the room, ask if you can draw inside the test booklet. Tell the proctor you like to make longhand notes when solving problems. Usually the booklet will never be reused, so you can mark in it all day long.

You can make notes to yourself in the booklet and mark your favorite answer and then just transfer the answer from the test booklet to the answer sheet. This technique really helps if you start jumping around or choose to skip a question for later. Consider drawing useful diagrams such as the OSI separation of duties model on the inside back cover of the booklet. The proctor will tell you that only answers on the answer sheet will count toward your score.

Stay Healthy by Choosing Where You Sit

If the person sitting behind you or next to you at the exam is coughing, appears to be sick, or repeatedly sneezing, ask to be moved. Research shows anyone within 15 feet can get sick from the airborne germ cloud. You should ask the test proctor to allow you to move to another seat. The proctor should say yes for health reasons. Sometimes a contagious person will arrive to take their exam rather than reschedule. Since the test proctor is not medically trained, they will not ask the person to leave due to liability. Forcing you to be exposed is a liability trap too. You should protect your own health instead of being polite. The person exposing you is being callous toward your health. Move.

Plan on Using All Four Hours

You should expect the test to take the entire four hours. Manage your time carefully to avoid running out of time before finishing the test. It is advisable to plan ahead for both pace and breaks. The exam proctor will usually allow you to take restroom breaks as long as you do not talk to anyone about the exam while out of the room. You might find it helpful to reduce fatigue by just taking a walk to the restroom and then splashing water on your face. One trip per hour seems to work fine. Most test takers will finish in the last 10 minutes before time is called by the proctor.

Read the Question Carefully

Read each question *very* carefully! The questions are intentionally worded differently from the questions in this study guide. If you come across overly confusing questions or ones that you are not sure of, try reading them twice or even three times.

On the first pass, circle the operative points in the question, such as the words *not*, *is*, *best*, *and*, *or*, and so on. Next, underline the nouns or the subject of the question. For example, if the question is "The purpose of controls is to…," you would underline *purpose* and circle the word *is*.

On the second pass, ensure that you understand the implied direction of the question and its subject. Does the question have a positive (*is*) or negative (*is not*) implication? Watch for meanings that are positive, negative, inclusive, or exclusive. A common technique used for writing test questions is to imply terminology associations that should not exist or to deny terminology associations that in fact exist. Do not violate the intent of the question or answer. Most people fail a question by misreading it.

On the third pass, dissect the available answers by using a similar method. Watch for conflicting meaning or wrong intent.

Place a star next to any question in the booklet for which you have doubts about your answer. You can return to the question before turning in your answer sheet. (This keeps your answer sheet clean of any stray marks.)

For your final check, you can compare the answers marked in the test booklet to your answer sheet. Remember that there is no penalty for wrong answers. Do not leave any blank. Just take a guess if you must. A sample video of question-reading techniques is on the companion website.

Done! The Exam Is Over

Plan for a relaxing activity with your family or friends after the exam. We suggest you plan something that is fun and doesn't require mental concentration; you will be mentally worn out after the exam. Do not punish yourself by looking up the answers for a particular test question. The test is over. Now it's time to enjoy yourself.

The folks at CertTest wish you all the best. Good luck on your exam.

Getting Your CISA Awarded

A notice of your official letter with overall score will be mailed or emailed to you five to eight weeks after the exam. You should expect the mailed letter to be only two pages stating that you either failed or passed. ISACA will inform you of your score. Contesting a score is usually a waste of effort.

After you pass, the next step is to download and complete ISACA's application to be certified. You will need to provide contact names for your references, complete with email addresses and phone numbers. Each reference will need to sign a form indicating your experience and check the box stating that you would be an asset to the audit profession. It's your job to mail these forms back to ISACA along with your application for certification. ISACA will verify your claim prior to awarding you the CISA credential. No reference = no credit. Inform your references in advance so they are ready to respond to ISACA's reference check. It's a good idea to have lunch with your references in advance. Give them a copy of your CISA application and discuss it with them in person. You can expect to be an official CISA 10 to 12 weeks after the exam—*if* you are prompt in filing the application and do a good job of managing the timely response of your references.

CISA Job Practice Areas

The ISACA objectives for CISA candidates are presented in this book using a slightly different order than how they are listed in ISACA's training materials for easier learning.

Chapter 1—Secrets of a Successful Auditor

The easiest way to help you learn quickly is to start with an orientation of the normal activities in the auditor's day. These activities cover answers to the top questions about

who, what, where, and why. This chapter covers topics such as why auditors don't trust people or systems until the test results indicate that they can, who's responsible for a particular task, why executives lie, and so on.

The first chapter includes some basic information about IS auditing to help you grasp the core points right away. These topics are in the exam but are not itemized separately in this chapter.

Domain 1—IS Audit Process (14%)

To provide IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.

Domain 1—The Process of Auditing Information Systems

Provide audit services in accordance with IS audit standards to assist the organization in protecting and controlling information systems. (21%)

Task Statements:

1.1	Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited.
1.2	Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
1.3	Conduct audits in accordance with IS audit standards to achieve planned audit objectives.
1.4	Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary.
1.5	Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner.

Knowledge Statements:

1.1	Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
1.2	Knowledge of the risk assessment concepts and tools and techniques used in planning, examination, reporting and follow-up
1.3	Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes
1.4	Knowledge of the control principles related to controls in information systems

1.5	Knowledge of risk-based audit planning and audit project management techniques, including follow-up
1.6	Knowledge of the applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits
1.7	Knowledge of the evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence
1.8	Knowledge of different sampling methodologies and other substantive/ data analytical procedures
1.9	Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification)
1.10	Knowledge of audit quality assurance (QA) systems and frameworks
1.11	Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Domain 2—Governance and Management of IT

Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy. (16%)

Task Statements:

2.1	Evaluate the IT strategy, including IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
2.2	Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
2.3	Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
2.4	Evaluate the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.

2.5 Evaluate IT resource management, including investment, prioritization, allocation and use, for alignment with the organization's strategies and objectives.

2.6 Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.

2.7 Evaluate risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.

2.8 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures.

2.9 Evaluate monitoring and reporting of IT key performance indicators (KPIs) to determine whether management receives sufficient and timely information.

2.10 Evaluate the organization's business continuity plan (BCP), including alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption.

Domain 3—Information Systems Acquisition, Development and Implementation

Provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the organization's strategies and objectives. (18%)

Task Statements:

3.1 Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether the business case meets business objectives.

3.2 Evaluate IT supplier selection and contract management processes to ensure that the organization's service levels and requisite controls are met.

3.3 Evaluate the project management framework and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the organization.

3.4 Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation, and has timely and accurate status reporting.

3.5 Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.

3.6 Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met.

3.7 Conduct post-implementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.

Domain 4—Information Systems Operations, Maintenance and Service Management

Provide assurance that the processes for information systems operations, maintenance and service management meet the organization's strategies and objectives. (20%)

Task Statements:

4.1 Evaluate the IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives are met.

4.2 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the enterprise architecture (EA).

4.3 Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives.

4.4 Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives.

4.5 Evaluate database management practices to determine the integrity and optimization of databases.

4.6 Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives.

4.7 Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analyzed, reported and resolved in a timely manner to support the organization's objectives.

4.8	Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented.
4.9	Evaluate end-user computing to determine whether the processes are effectively controlled and support the organization's objectives.
4.10	Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether they are controlled effectively and continue to support the organization's objectives.

Knowledge Statements:

4.1	Knowledge of service management frameworks
4.2	Knowledge of service management practices and service level management
4.3	Knowledge of the techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements
4.4	Knowledge of enterprise architecture (EA)
4.5	Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)
4.6	Knowledge of system resiliency tools and techniques (e.g., fault-tolerant hardware, elimination of single point of failure, clustering)
4.7	Knowledge of IT asset management, software licensing, source code management and inventory practices
4.8	Knowledge of job scheduling practices, including exception handling
4.9	Knowledge of the control techniques that ensure the integrity of system interfaces
4.10	Knowledge of capacity planning and related monitoring tools and techniques
4.11	Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
4.12	Knowledge of data backup, storage, maintenance and restoration practices
4.13	Knowledge of database management and optimization practices
4.14	Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)
4.15	Knowledge of problem and incident management practices

4.16	Knowledge of change management, configuration management, release management and patch management practices
4.17	Knowledge of the operational risk and controls related to end-user computing
4.18	Knowledge of the regulatory, legal, contractual and insurance issues related to disaster recovery
4.19	Knowledge of business impact analysis (BIA) related to disaster recovery planning
4.20	Knowledge of the development and maintenance of disaster recovery plans (DRPs)
4.21	Knowledge of the benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)
4.22	Knowledge of disaster recovery testing methods
4.23	Knowledge of the processes used to invoke the disaster recovery plans (DRPs)

Domain 5—Protection of Information Assets

Provide assurance that the organization's policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets. (25%)

Task Statements:

5.1	Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.
5.2	Evaluate the design, implementation, maintenance, monitoring and reporting of physical and environmental controls to determine whether information assets are adequately safeguarded.
5.3	Evaluate the design, implementation, maintenance, monitoring and reporting of system and logical security controls to verify the confidentiality, integrity and availability of information.
5.4	Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
5.5	Evaluate the processes and procedures used to store, retrieve, transport and dispose of assets to determine whether information assets are adequately safeguarded.
5.6	Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.

Knowledge Statements:

5.1	Knowledge of the generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets
5.2	Knowledge of privacy principles
5.3	Knowledge of the techniques for the design, implementation, maintenance, monitoring and reporting of security controls
5.4	Knowledge of the physical and environmental controls and supporting practices related to the protection of information assets
5.5	Knowledge of the physical access controls for the identification, authentication and restriction of users to authorized facilities and hardware
5.6	Knowledge of the logical access controls for the identification, authentication and restriction of users to authorized functions and data
5.7	Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems) and database management systems.
5.8	Knowledge of the risk and controls associated with virtualization of systems
5.9	Knowledge of the risk and controls associated with the use of mobile and wireless devices, including personally owned devices (bring your own device [BYOD])
5.10	Knowledge of voice communications security (e.g., PBX, Voice-over Internet Protocol [VoIP])
5.11	Knowledge of network and Internet security devices, protocols and techniques
5.12	Knowledge of the configuration, implementation, operation and maintenance of network security controls
5.13	Knowledge of encryption-related techniques and their uses
5.14	Knowledge of public key infrastructure (PKI) components and digital signature techniques
5.15	Knowledge of the risk and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs, cloud computing)
5.16	Knowledge of the data classification standards related to the protection of information assets

5.17	Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
5.18	Knowledge of the risk and controls associated with data leakage
5.19	Knowledge of the security risk and controls related to end-user computing
5.20	Knowledge of methods for implementing a security awareness program
5.21	Knowledge of information system attack methods and techniques
5.22	Knowledge of prevention and detection tools and control techniques
5.23	Knowledge of security testing techniques (e.g., penetration testing, vulnerability scanning)
5.24	Knowledge of the processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
5.25	Knowledge of the processes followed in forensics investigation and procedures in collection and preservation of the data and evidence (i.e., chain of custody).
5.26	Knowledge of the fraud risk factors related to the protection of information assets

The ISACA Domains and the Real World

Always remember that the ISACA domains are an arbitrary division of the workflow. The ISACA separation of domains has a tendency to misrepresent the real-world correlations you would normally encounter in your daily work. In this book, I ignored ISACA's domains to help improve your understanding in easy-to-read segments.

If you are taking the exam, remember that questions will *never* follow the domain boundaries because the real workflow has no such arbitrary domain boundaries. Questions will span across the domains and the information provided in this book's chapters. To best prepare for the exam and the real world, you should read this book in the sequence in which it is presented.

The official and most up-to-date CISA job practice areas can be found at ISACA's website here:

`www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Job-Practice-Areas/Pages/CISA-Job-Practice-Areas.aspx`

Assessment Test

1. Which of these choices is the *best* answer regarding who is primarily responsible for providing internal controls to detect, correct, and prevent irregularities or illegal acts?
   - **A.** Board of directors
   - **B.** Information technology
   - **C.** Legal, aka general council
   - **D.** Human resources
2. Which of the following functions should be separated from the others if segregation of duties cannot be achieved in an automated system?
   - **A.** Origination
   - **B.** Authorization
   - **C.** Reprocessing
   - **D.** Transaction logging
3. What is the purpose of the audit committee?
   - **A.** To provide daily coordination of all audit activities
   - **B.** To challenge and review assurances
   - **C.** To assist the managers with training in auditing skills
   - **D.** To govern, control, and manage the organization
4. What are the qualifications of the incident commander when responding to a crisis?
   - **A.** Trained crisis manager
   - **B.** First person on scene
   - **C.** Member of management
   - **D.** First responder
5. Which of the following options is *not* true in regard to configuring routers, servers, workstations, printers, and networked databases set up using default settings?
   - **A.** Designed to reduce technical support during installation for novice users
   - **B.** Sufficient controls to provide a minimum level of safety for production use
   - **C.** Predictable to facilitate successful intrusion attacks using well-known filenames, access paths, and missing or incomplete security parameters
   - **D.** Remote scanning and automated penetration tools that prey upon systems running on default settings
6. How should management act to best deal with emergency changes?
   - **A.** Emergency changes cannot be made without advance testing.
   - **B.** The change control process does not apply to emergency conditions.
   - **C.** All changes should still undergo review.
   - **D.** Emergency changes are not allowed under any condition.

7. Which of the following would be a concern that the auditor should explain in the audit report along with their findings?
   - **A.** Lack of a detailed list of audit objectives
   - **B.** Undue restrictions placed by management on evidence use or audit procedure
   - **C.** Communicating results directly to the chairperson of the audit committee
   - **D.** Need by the current auditor to communicate with the prior auditors

8. During the performance of an audit, a reportable finding is identified with the auditee. The auditee immediately fixed the problem upon identification. Which of the following is true as a result of this interaction?
   - **A.** Auditee resolved the problem before the audit report is written, therefore no finding exists.
   - **B.** Auditor can verify that the corrective action has been taken before the audit report is written, therefore no finding exists.
   - **C.** Auditor includes the finding in the final audit report as resolved.
   - **D.** Auditor lists the finding as it existed.

9. Which of the following management methods provides the most control rather than discretionary flexibility?
   - **A.** Distributed
   - **B.** Centralized
   - **C.** In-house
   - **D.** Outsourced

10. What is the principal issue surrounding the use of CAAT software?
   - **A.** The capability of the software vendor
   - **B.** Documentary evidence is more effective
   - **C.** Inability of automated tools to consider the human characteristics of the environment
   - **D.** The possible cost, complexity, and security of output

11. Digital signatures are designed to provide additional protection for electronic messages in order to determine which of the following?
   - **A.** Message read by unauthorized party
   - **B.** Message sender verification
   - **C.** Message deletion
   - **D.** Message modification

12. Which is the primary benefit of using a risk-based approach in audit planning?
   - **A.** Simplifies resource scheduling.
   - **B.** Allocates resources to the areas of highest concern.
   - **C.** Properly trained personnel are available.
   - **D.** Lowers the overall cost of compliance.

13. What indicators are used to identify the anticipated level of recovery and loss at a given point in time?
    - **A.** RPO and RTO
    - **B.** RTO and SDO
    - **C.** RPO and ITO
    - **D.** SDO and IRO

14. Which of the following is the *best* choice to ensure that internal control objectives are met?
    - **A.** Top executive issues a policy stating compliance objectives.
    - **B.** Procedures are created to govern employee conduct.
    - **C.** Suitable systems for tracking and reporting incidents are used.
    - **D.** The clients operating records are audited annually.

15. Which of the following statements is true concerning asymmetric key cryptography?
    - **A.** The sender encrypts the files by using the recipient's private key.
    - **B.** The sender and receiver use the same key.
    - **C.** Asymmetric keys cannot be used for digital signatures.
    - **D.** The sender and receiver have different keys.

16. Who is responsible for designating the appropriate information classification level?
    - **A.** Data custodian
    - **B.** Data user
    - **C.** Data owner
    - **D.** Security manager

17. What is the *best* statement regarding the purpose of using the OSI model?
    - **A.** To define separation of duties, controls, and boundaries
    - **B.** To define which level of program-to-program gateways operate
    - **C.** To define how networking protocols work for IT professionals
    - **D.** To define the differences between OSI and IP protocols

18. What is one of the bigger concerns regarding asset disposal?
    - **A.** Residual asset value
    - **B.** Employees taking disposed property home
    - **C.** Standing data
    - **D.** Environmental regulations

19. What is the primary purpose of database views?
    - **A.** Restrict the viewing of selected data
    - **B.** Provide a method for generating reports
    - **C.** Allow the user access into the database
    - **D.** Allow the system administrator access to maintain the database

20. Which step is necessary before moving into the next phase when using the System Development Life Cycle?

A. Phase meeting

B. Change control

C. Formal approval

D. Review meeting

21. Which of the following indicates why continuity planners can create plans without a business impact analysis (BIA)?

A. Management already dictated all the key processes to be used.

B. They can't because critical processes may change monthly or annually.

C. Business impact analysis is not required.

D. Risk assessment is acceptable.

22. Which of the following answers contains the steps for business process reengineering (BPR) in proper sequence?

A. Diagnose, envision, redesign, reconstruct

B. Envision, initiate, diagnose, redesign, reconstruct, evaluate

C. Evaluate, envision, redesign, reconstruct, review

D. Initiate, evaluate, diagnose, reconstruct, review

23. Segregation or separation of duties may not be practical in a small environment. A single employee may be performing the combined functions of server operator and application programmer. The IS auditor should recommend controls for which of the following?

A. Automated logging of changes made to development libraries

B. Procedures that verify that only approved program changes are implemented

C. Automated controls to prevent the operator logon ID from making program modifications

D. Hiring additional technical staff to force segregation of duties

24. Which of the following is true concerning reporting by internal auditors?

A. Results can be used for industry licensing.

B. The corresponding value of the audit report is high.

C. Results can be used for external reporting.

D. The corresponding value of the audit report is low.

25. The auditor is permitted to deviate from professional audit standards when they feel it is necessary because of which of the following?

A. Standards are designed for discretionary use.

B. The unique characteristics of each client will require auditor flexibility.

C. Deviating from standards is almost unheard of and would require significant justification.

D. Deviation depends on the authority granted in the audit charter.

26. Which of the following is true regarding the principle of auditor independence?

- **A.** It is not an issue for auditors working for a consulting company.
- **B.** It is required for an external audit to prevent bias.
- **C.** An internal auditor must undergo certification training to be independent.
- **D.** The audit committee would bestow independence on the auditor.

27. What is the best definition of *auditing*?

- **A.** Review of past history using evidence to tell the story
- **B.** Forecasting compliance generated by a new system preparing to enter production
- **C.** Precompliance assessment based on management's intended design
- **D.** Certification testing of the system benefits or failures

28. Which of the following is the most significant issue to consider regarding insurance coverage?

- **A.** Premiums may be very expensive.
- **B.** Insurance can pay for all the costs of recovery.
- **C.** Coverage must include all business assets.
- **D.** Salvage, rather than replacement, may be dictated.

29. Which of the following statements is *not* true regarding the use of passwords for authentication?

- **A.** Password lockout is not effective against hackers using the common technique of bypassing the login utility.
- **B.** Hash utilities for one-way encryption of OS login passwords are highly susceptible to chosen ciphertext lookup tables, which will show the actual plaintext password currently in use.
- **C.** Many dynamic websites with a database backend use program-to-program configuration files to store the passwords using encrypted hash format.
- **D.** Passwords are portable, easily captured and reused for unauthorized access, and considered terribly weak authenticators.

30. Using public-key interchange (PKI) encryption, which key is used by the sender for authentication of the receiving party?

- **A.** Sender's private key
- **B.** Recipient's private key
- **C.** Recipient's public key
- **D.** Sender's public key

31. Which of the following statements is true concerning a software worm?

- **A.** Uses authentication defects to freely travel to infect other systems
- **B.** Is a synonym for a malicious virus appending itself to data files
- **C.** Must be executed by opening a file
- **D.** Attaches itself to programs and data by the opening and closing of files

32. What are three of the four key perspectives on the IT balanced scorecard?

A. Business justification, service-level agreements, budget

B. Organizational staffing, cost reduction, employee training

C. Cost reduction, business process, growth

D. Service level, critical success factors, vendor selection

33. Which sampling method is used when the likelihood of finding evidence is low?

A. Discovery

B. Cell

C. Random

D. Stop and go

34. Which of the following would represent the greatest concern to an auditor investigating roles and responsibilities of the IT personnel?

A. An IT member is reviewing current server workload requirements and forecasts future needs.

B. An IT member monitors system performance, making necessary program changes and tracking any resulting problems.

C. An IT member tests and assesses the effectiveness of current procedures and recommends specific improvements.

D. An IT member works directly with the user to improve response times and performance across the network.

35. When auditing the use of encryption, which of the following would be the primary concern of the auditor?

A. Management's level of control over the use of encryption

B. Strength of encryption algorithm in use

C. Key sizes used in the encryption and decryption process

D. Using the correct encryption method for compliance

36. Which of the following represents the hierarchy of controls from highest level to lowest level?

A. General, pervasive, detailed, application

B. Pervasive, general, application, detailed

C. Detailed, pervasive, application, detailed

D. Application, general, detailed, pervasive

37. What is the primary objective in the third phase of incident response?

A. Containment

B. Lessons learned

C. Eradication

D. Analysis

38. What is the purpose of using the ACID principle with database applications?

A. To write the entire transaction to the master file or discard without making any changes

B. To provide environmental protection to safeguard the server to ensure maximum uptime

C. To step-link each data transaction to ensure consistency

D. To remove unnecessary data from the database for better performance

39. What is the first priority of management upon the possible detection of an irregular or illegal act?

A. Shut down access to the system.

B. Aid the process of investigation and inquiry.

C. Notify appropriate law enforcement.

D. Contact auditors to schedule an audit of the situation.

40. What is the principle purpose of using function point analysis?

A. Verify the integrity of financial transaction algorithms in a program

B. Estimate the complexity involved in software development

C. Review the results of automated transactions meeting criteria for the audit

D. Provide system boundary data during the Requirements Definition phase

41. Which of the following common methods is typically *not* used by hackers to remotely control encryption keys which exist unencrypted in executable RAM memory?

A. Malware downloading and installing a Trojan horse utility without the user's knowledge

B. Remotely gaining unencrypted access to POS/computers on the internal store LAN before encryption occurs for transmission

C. Gaining physical access into the system using social engineering

D. Gaining unauthorized access using static passwords in configuration files intended for program-to-program access

42. Which of the following is not one of the three major control types?

A. Detective

B. Deterrent

C. Preventive

D. Corrective

43. Which method of backup should be used on a computer hard disk or flash media prior to starting a forensic investigation?

A. Full

B. Differential

C. Bitstream

D. Logical

44. After presenting the report at the conclusion of an audit, the lead auditor discovers the omission of a procedure. What should the auditor do next?

A. Log on to `CareerBuilder.com` and change their current employment status to available.

B. Cancel the report if audit alternatives cannot compensate for the deficiency.

C. File an incident disclosure report with the audit association to minimize any liability.

D. No action is required as long as the omitted procedure is included in the next audit.

45. Which of the following statements is *not* true regarding devices or systems that routinely allow unknown or unauthenticated users access to use the CPU, memory, or hard drive storage?

A. Unknown/anonymous users can upload or download data from the web server database. Unintended data or configuration settings may be revealed or executable code with escalation attack commands may be uploaded.

B. Unknown/anonymous users can access the LAN printer/multi-function device (MFP) to spool, print, fax, or receive files or remotely manipulate device settings.

C. Unknown/anonymous users can remotely alter startup settings or boot file images without the knowledge of system administrators.

D. Unknown/anonymous users can be sales prospects, so the risk is acceptable because security controls must be cost effective and not interrupt revenue activities.

46. In regard to the IT governance control objectives, which of the following occurrences would the auditor be most concerned about during execution of the audit?

A. Using the practice of self-monitoring to report problems

B. Using proper change control

C. Conflict in the existing reporting relationship

D. Production system without accreditation

47. What is the purpose behind system accreditation?

A. Hold management responsible for fitness of use and any failures

B. Provide formal sign-off on the results of certification tests

C. Improve the accuracy of forecasting in IT budgets

D. Make the user responsible for their use of the system

48. Implementing a strong external boundary is a successful method to prevent hackers and thieves from accessing your internal computer systems provided you are using which of the following technologies?

A. Internet firewalls and intrusion detection systems with prevention capabilities (an IDPS) to prevent ingress

B. Strong administrative policy controls with harsh sanctions that include termination and/or criminal liability

C. Antivirus software with malware detection capabilities

D. The elimination of shared access accounts and static passwords, including those shared for mandatory administrative access

49. Which of the following techniques is used in the storage and transmission of a symmetric encryption key?

A. Key rotation

B. Generating a unique encryption key

C. Key wrapping

D. Generating a shared encryption key

50. Which of the following situations should the auditor consider if the auditee has implemented six phases of the System Development Life Cycle (SDLC)?

A. The auditee is probably doing a good job with no concerns at this time.

B. The IT governance model has been implemented.

C. The auditee may be missing a critical function.

D. There are only five phases to the System Development Life Cycle.

51. Which backup method will copy only changed files without resetting the archive bit (archive flag)?

A. Physical

B. Incremental

C. Full

D. Differential

52. What is the purpose of a digital signature?

A. Electronic marker showing the recipient that a sender actually sent a document

B. Provides a copy of the sender's public key along with the document

C. Cyclic redundancy check to prove document integrity

D. Provides the recipient with a method of testing the document received from a sender

53. What is the functional difference between *identification* and *authentication*?

A. Authorization is a match; identification is only a claim until verified.

B. Authentication is only a claim; identification is a verified match.

C. Identification is only a claim until verified; authentication is a match.

D. Identification is only a claim; authorization is a match.

54. Select the best answer to finish this statement: A _____ is strategic in nature, while the _____ is tactical.

A. policy, procedure

B. standard, procedure

C. procedure, standard

D. policy, standard

55. What is the primary objective for using a system with a Redundant Array of Independent—or Inexpensive—Disks (RAID)?

A. Prevent corruption

B. Increase availability

C. Eliminate the need for backups

D. Increase storage capacity

56. What function does the auditor provide?

A. Second set of eyes, which are external to the subject under review

B. Independent assurance that the claims of management are correct

C. Assistance by fixing problems found during the audit

D. Adapting standards to fit the needs of the client

57. Which of the following situations does *not* represent a reporting conflict?

A. Information security manager reporting to internal auditors

B. Employee reporting violations to their boss, who is also in charge of compliance

C. IT security reporting to the chief information officer

D. Self-monitoring and reporting of violations

58. Complete the following statement with the best available answer: The _____ file is created when the system shuts down improperly. It usually contains _____ that is/are useful in forensic investigations or used by hackers to leak confidential data and your authenticators.

A. dump, contents from RAM memory

B. abend, a history of all the user transactions processed

C. diagnostic, system startup settings

D. abort, all user account information

59. In using public-key interchange (PKI) encryption, which key is *not* used by the recipient for decrypting a message?

A. Sender's private key

B. Recipient's private key

C. Sender's public key

D. Recipient's public key

60. Where should the computer room be located?

A. Secure basement

B. First floor

C. Middle floor

D. Top floor

61. What is the primary purpose of using the root kit?

- **A.** System administration tool used by the superuser, also known as the server agent
- **B.** Method for tracing source problems in determining cause-and-effect analysis
- **C.** Camouflage technique designed to hide certain details from view
- **D.** Covert method of remotely compromising the operating system kernel

62. Complete the following statement: A _____ must be used to prevent _____ of the hard-disk evidence during the collection phase of forensic investigations.

- **A.** forensic specialist, analysis
- **B.** write blocker, contamination
- **C.** immunizer, corruption
- **D.** data analyzer, destruction

63. Which of the following statements is true concerning the role of management and the role of the auditor?

- **A.** Management uses the auditor's report before making their assertions.
- **B.** Management must make their assertions prior to reading the auditor's report.
- **C.** The auditor is able to view only evidence that has been predetermined by management.
- **D.** The auditor's opinion will be based on the desire of management.

64. Which of the following is the best way for an auditor to prove their competence to perform an audit?

- **A.** Having prior experience working in information technology
- **B.** Citing each point in a regulation with an audit objective and specific test
- **C.** Obtaining auditor certification with ongoing training
- **D.** Having prior experience in financial auditing

65. Which of the following processes would be the best candidate for business process reengineering?

- **A.** Excluded process
- **B.** Nonworking process
- **C.** Working process
- **D.** Marginal process

66. Which of the following statements is true concerning the auditor's qualified opinion?

- **A.** The auditor has reservations about the findings.
- **B.** The auditor is professionally qualified to give an opinion.
- **C.** The auditor has no reservations about the findings.
- **D.** The auditor has prior experience working in the IT department.

67. Wireless LAN encryption systems using Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA, WPA2-PSK) in the transmission of network data will base the transmission security upon which of the following?

A. Broadcasting a single password through the airwaves to be shared by all network users

B. Broadcasting a unique individual password for each of the network users

C. Strength of the WPA2 encryption algorithm selected during the configuration at setup

D. Strength of the encryption key being used with WPA2

68. During a business continuity audit, it is discovered that the business impact analysis (BIA) was not performed even though an initial feasibility review of the financial statement was performed. What would this indicate to the auditor?

A. The customer was able to get their plan in place without using the BIA technique.

B. The business continuity plan is likely to be a failure.

C. Risk analysis and the customer's selection of the strategy fulfill their most important objectives.

D. It's not necessary to perform a business impact analysis because financial feasibility was performed.

69. Which of the following systems uses heuristic techniques to make decisions on behalf of the user?

A. Associate decision mart

B. Expert system

C. Decision support system (DSS)

D. Data warehouse

70. Which of the following is the best representation of a soft token used for two-factor authentication?

A. Digital signature

B. Digital identity

C. Digital certificate

D. Digital hash

71. Which of the following is the best example of implementing a detective control via administrative methods?

A. Auditing of system configuration and log files

B. Running a verification of the backup tape for integrity

C. Using an intrusion detection and prevention system (IDPS)

D. Restoring a damaged file using a copy from the vendor