Introduction

Welcome! Whether this is your first Exam Prep series book or your fifteenth, you will find information here that will help ensure your success as you pursue knowledge, experience, and certification. This introduction explains the Information Systems Audit and Control Association (ISACA) certification program and discusses the way this Exam Prep book can help you prepare for the Certified Information Systems Auditor (CISA) exam. In particular, this introduction discusses the basics of ISACA certification exams and describes the test-taking environment and test-taking strategies. Chapters 1–9 are designed to help you study and prepare for the exam. Next, a Fast Facts section provides a high-level overview of exam objectives; finally, you'll find a full-length exam at the end of the book to give you a reasonable assessment of your knowledge. This book also provides the answers and explanations to the practice exam so you can go back and review why you missed specific questions or better understand the rationale of specific questions. If you read this book, study the material, and review the practice test, you will have a good chance of passing the actual exam.

How This Book Helps You

Exam Prep books are designed to help you understand and appreciate the subjects and materials you need to pass the ISACA CISA certification exam. The Exam Prep series is aimed strictly at test preparation and review. You will not learn the intricate details about everything there is to know about a specific topic because the assumption is that you have either on-the-job experience or coursework in the past that makes you eligible as a CISA certification candidate. This book is designed to present you with the material and topics you are likely to find on the actual test. We've worked to bring together as much information as possible about the CISA exam.

With this in mind, you still should make sure you are fully prepared for the exam and also have the subsequent skills that an employer might ask you to perform with such a certification. This might mean that in addition to reading the book, you also attend classroom training, gain hands-on practice auditing systems, or read one or more complementary texts, including the award-winning certification preparation series from Que Publishing. We recommend that you supplement your study program with visits to http://www.examcram.com to receive additional practice questions, get advice, and track the CISA program.

About the CISA Exam

The Information Systems Audit and Control Association (ISACA) developed the Certified Information Systems Auditor (CISA) program in 1978 to accomplish the following goals:

- Develop and maintain a testing instrument that can be used to evaluate an individual's competency in conducting information systems audits
- Provide a mechanism for motivating systems auditors to maintain their competencies and monitoring the success of the maintenance programs
- Aid top management in developing a sound information systems audit function by providing criteria for personnel selection and development

The CISA program is designed to assess and certify individuals in the IS audit, control, or security profession who demonstrate exceptional skills judgment and proficiency in IS audit control and security practices.

More than 50,000 professionals have earned the certification since its creation, and it is widely recognized as the premier information systems auditing certification.

This number is sure to grow as the U.S. Department of Defense (DoD) 8570.01-M *Information Assurance Workforce Improvement Program* manual names ISACA's Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certifications among those approved for DoD information assurance (IA) professionals. This IT-based directive requires up to 80,000 professionals to earn one of 13 certifications offered by five organizations.

CISA Exam Objectives

The CISA exam is divided into six job practice areas, each of which is weighted differently. Table I.1 lists and describes the different job practice areas and provides the percentage of the exam pulled from each area.

TABLE I.1 CISA Exam Job Practice Areas and Breakdown

Job Practice Area	Title	Description	Percentage of Exam
Area 1	**IS Audit Process**	The IS Audit Process job practice area describes the IS audit services in accordance with IS audit standards, guidelines, and best practices. These services are provided to assist the organization in ensuring that its information technology and business systems are protected and controlled.	10%

TABLE I.1 *Continued*

Job Practice Area	Title	Description	Percentage of Exam
Area 2	**IT Governance**	The IT Governance job practice area describes the assurance controls that the organization has in place, such as structure, policies, accountability, mechanisms, and monitoring to control the practices of IT.	15%
Area 3	**Systems and Infrastructure Lifecycle**	The Systems and Infrastructure Lifecycle job practice area describes controls used to meet organizational objectives in the development/acquisition, testing, implementation, maintenance, and disposal of information systems and infrastructure.	16%
Area 4	**IT Service Delivery and Support**	The IT Service Delivery and Support job practice area discusses the practices used to ensure the delivery of the level of services required to meet the organization's objectives in providing assurance to IT service management.	14%
Area 5	**Protection of Information Assets**	The Protection of Information Assets job practice area ensures the confidentiality, integrity, and availability of information assets by means of the security architecture (policies, standards, procedures, and related controls).	31%
Area 6	**Business Continuity and Disaster Recovery**	The Business Continuity job practice area takes into consideration IT and critical business services. Disaster Recovery describes the controls used to reduce the impact of a disruption and minimize these events to ensure a timely resumption of IT services.	14%

You can review a complete breakdown of the CISA exam objectives at http://www.isaca.org/Template.cfm?Section=Content_Areas&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20418.

How to Prepare for the Exam

The CISA exam is somewhat difficult to prepare for because it is so broad in scope. It is also challenging because it asks indirect questions that require strong cognitive skills. The exam format is also something that most test takers are not familiar with—it is paper-based, not computerized, and is presented as 200 multiple-choice questions prepared in booklet form. Individuals attempting the exam are required to fill in the bubble on the basic Scantron-type answer sheet.

Don't think that this is an exam that you can adequately prepare for by simply memorizing terms and definitions. The questions presented by the CISA exam require you to analyze facts

from various domains and knowledge points. Synthesizing this information requires giving thought and analysis to various factors in concluding what is the best answer from several possible answers. Having passed exams such as the CISM, CISSP, SCNP, CCSE, and others will help when analyzing questions and related material.

Additional Exam-Preparation Resources

Because the scope of the exam is so broad, it would not be hard to spend months or even years preparing for the exam. Although it would be helpful to read the hundreds of books that some might recommend preparing for the exam, this is not always feasible. This points to one of the reasons this book was created. However, those preparing for the exam have other resources available as well. Your decisions to use these materials will be driven largely on a case-by-case basis: Some individuals have many years of experience in many domains, whereas others may have focused on only one or two and have little knowledge in the other CISA domains. Some of the additional resources available include the following:

- ***The CISA Review Manual***—This book is available at http://www.isaca.org. The official review manual is for students to review the type of content that can be found on the exam. Although this is a good supplementary resource, do not expect it to provide 100% coverage of what is needed for the exam.
- **The CISA Review Questions and Answers CD-ROM**—This good—yet expensive—resource offers practice questions for review. Although it will give you some additional questions that are of the same structure as those on the actual exam, do not expect to see much overlap between these questions and the real exam. This resource is also available at http://www.isaca.org.
- **Instructor-led training**—Instructor-led training is another option for those preparing for the exam. Some ISACA chapters provide review seminars to help those preparing for the exam. These sessions are generally reasonably priced. Just keep in mind that although ISACA provides the overall template for the review sessions, the individual chapters have the final say on how these are delivered. It's also worth noting that a volunteer instructor provides the instruction, so the quality, presentation skills, and amount of time the instructor has spent preparing for the class will vary.

Other professional training organizations also offer CISA training. The author of this book works for one such company, Superior Solutions, Inc. As president of the company, he has led the development of its CISA training material and often teaches the class. This specialized curriculum focuses on the core essentials of IT audit and IT governance best practices. Superior Solutions, Inc., provides these classes throughout the world. If you feel that you need more than an exam guide and are looking for instructor-led training, take a moment to look over the Superior Solutions, Inc., course offerings at http://www.thesolutionfirm.com.

Practice Tests

You do not need to know much about practice tests other than that they are a worthwhile expense, for three reasons:

- They help you diagnose areas of weakness.
- They help you get used to the format of questions.
- They help you determine when you are ready to take the exam.

This book contains questions at the end of each chapter and also includes a full-length practice test. ISACA is one source for additional practice questions, and many other companies provide CISA certification practice tests (of course, their quality is an unknown factor).

What This Book Does

This book is designed to point you to the topics and subjects that the CISA exam will cover. The book is designed to be used early on, well before the test, to give you insight on how comprehensive your knowledge is of the various topics. This might be enough for some readers; others might then need to research some material to get a deeper understanding of a specific topic. For example, you might read about CobiT and realize that you have very little knowledge about this framework, and then visit http://www.isaca.org to read more about the subject.

This book is also designed to be used as a final review. Perhaps you have attended a review seminar or instructor-led training but would like one more review before attempting the exam. In that case, this book distills the various topics for you, giving you a complete review of each in as few pages as possible. Exam Alerts, bullet points, study review points, and chapter reviews will all help build that level of confidence and knowledge needed to pass the exam on the first try.

As the author of this book, I developed the material from my experience teaching many students around the world, from my review of the official guide, from personal knowledge of the material, and from a battery of third-party test tools and websites. Apart from the actual logical step-by-step learning progression of the chapters themselves, this book—and all *Exam Prep* books—uses elements such as Exam Alerts, tips, notes, and practice questions to make the information easier to read and absorb.

Most people seeking certification use multiple sources of information. Check out the links at the end of each chapter to get more information about subjects with which you might not have as much experience. Practice tests can help indicate when you are ready. You can also find a variety of security and audit books that deal with many of the other topics, discussed in much greater detail. Don't forget that many individuals have described the CISA exam as being very

challenging! Some ISACA chapters report only a 60–70 percent first-time pass rate. The CISA exam assumes that you already have a strong background in information system auditing and controls. This book helps you fill in the gaps.

What This Book Does Not Do

Now that you know what this book provides, it is only fair to cover what the book does not do. Primarily, this book will not teach you all you need to know about auditing systems and controls. The book is also not designed to be an introduction to computer technology. This book focuses on what you need to know to prepare for and pass the CISA exam.

The targeted reader for this book is someone seeking CISA certification. However, it should be noted that an *Exam Prep* book is an easily readable rapid presentation of facts. Therefore, an *Exam Prep* book is also extremely useful as a quick-reference manual.

Contacting the Author

The goal of this book is to provide you with the best prep possible. I am interested in any feedback you would like to share about the book. I would like to know any ideas you have on how it could be improved. Hopefully this book provides you with the tools you need to pass the CISA exam. You can contact me at the following email address:

info@thesolutionfirm.com

Finally, thank you for selecting my book; I hope you like it. If you have a moment, please email and let me know what you thought your chances of passing the test were before you read the book and after you read the book. Most of all, I would love to hear that you passed the exam. It always feels good to share personal successes with others. Good luck!

About the Book

This book is organized by individual exam objectives; it covers every objective you need to know for the CISA exam. We have attempted to present the objectives in an order that is as close as possible to that listed by ISACA. However, we have not hesitated to reorganize them where needed to make the material as easy as possible for you to learn. Some job practice areas of content are much larger than others, so we have broken them up into digestible elements. The list shown here outlines the basic structure of the chapters as they map to the CISA areas of knowledge:

- Part I: The Audit Process
  - Chapter 1: The Audit Process
- Part II: IT Governance
  - Chapter 2: IT Governance
- Part III: System and Infrastructure Lifecycle Management
  - Chapter 3: Lifecycle Management
  - Chapter 4: System Infrastructure Control
- Part IV: IT Service Delivery and Support
  - Chapter 5: Information Systems Hardware and Architecture
  - Chapter 6: Information Systems Used for IT Delivery and Support
- Part V: Protection of Information Assets
  - Chapter 7: Protection of Logical Assets
  - Chapter 8: Physical Security
- Part VI: Business Continuity and Disaster Recovery
  - Chapter 9: Business Continuity and Disaster Recovery

We have also attempted to make the information accessible in the following ways:

- The Exam Objectives Reference element of the book gives the full list of job practice areas and tasks and knowledge statements.
- Each chapter begins with a list of the tasks and knowledge statements to be covered.
- Each chapter also begins with an outline that provides you with an overview of the material and the page numbers where particular topics can be found.
- The tasks and knowledge statements are repeated where the material most directly relevant to it is covered.

Instructional Features

This book has been designed to provide you with multiple ways to learn and reinforce the exam material. The following are some of the helpful methods:

- **Study and Exam Preparation Tips**—You should read this section early on, to help develop study strategies. This section also provides you with valuable exam-day tips

and information on exam/question formats such as adaptive tests and case study–based questions.

- **Objective explanations**—As mentioned previously, each chapter begins with a list of the tasks and knowledge statements (collectively referred to as objectives) covered in the chapter. In addition, immediately following each objective is an explanation of the objective, in a context that defines it meaningfully.
- **Study strategies**—The beginning of each chapter also includes strategies for approaching the studying and retention of the material in the chapter, particularly as it is addressed on the exam, but also in ways that will benefit you on the job.
- **Exam Alerts**—Exam Alerts provide specific exam-related advice. Such tips might address what material is covered (or not covered) on the exam, how it is covered, mnemonic devices, or particular quirks of that exam.
- **Review breaks and summaries**—Crucial information is summarized at various points in the book in lists or tables. Each chapter ends with a summary as well.
- **Key terms**—A list of key terms appears at the end of each chapter.
- **Notes**—Notes contain various kinds of useful or practical information, such as tips on technology or administrative practices, historical background on terms and technologies, or side commentary on industry issues.
- **Warnings**—When using sophisticated information technology, the potential for mistakes or even catastrophes because of improper application of the technology always exists. Warnings alert you to such potential problems.
- **"In the Field" sidebars**—These relatively extensive discussions cover material that might not be directly relevant to the exam but that is useful as reference material or in everyday practice. "In the Field" sidebars also provide useful background or contextual information that is necessary for understanding the larger topic under consideration.
- **Exercises**—Found at the end of the chapters in the "Apply Your Knowledge" section and in the Challenge Exercises found throughout chapters, exercises are performance-based opportunities for you to learn and assess your knowledge.

Extensive Practice Test Options

The book provides numerous opportunities for you to assess your knowledge and practice for the exam. The practice options include the following:

- **Exam questions**—These questions appear in the "Apply Your Knowledge" section within each chapter. You can use them to help determine what you know and what you

need to review or study further. Answers and explanations for these questions are provided in a separate section, titled "Answers to Exam Questions," later in each chapter.

- **Practice exam**—A practice exam is included in the "Final Preparation" section of the book.

Final Preparation

The Final Preparation part of the book provides three valuable tools for preparing for the exam:

- **Fast Facts**—This condensed version of the information contained in the book is extremely useful for last-minute review.
- **Practice exam**—Questions on this practice exam are written in styles similar to those used on the actual exam. You should use the practice exam to assess your readiness for the real thing.
- **Practice exam answers**—Use the extensive answer explanations to improve your retention and understanding of the material.

The book includes several other features, such as a section titled "Need to Know More" at the end of each chapter that directs you to additional information that can aid you in your exam preparation and your real-life work, and a glossary.

For more information about the exam or the certification process, refer to the ISACA website at http://www.isaca.org.

Final Words of Wisdom

More extensive tips are found in the "Study and Exam Prep Tips" section, but keep this advice in mind as you study:

- **Read all the material**—ISACA has been known to include complex wording or create questions in ways that will make the reader search for pertinent facts. This book includes additional information that is not reflected in the objectives, in an effort to give you the best possible preparation for the examination—and for your real-world experiences to come.
- **Complete the exercises in each chapter**—They will help you gain experience and aid in gaining real-life skills so that you can apply the knowledge learned.

- **Use the exam questions to assess your knowledge**—Don't just read the chapter content; use the exam questions to find out what you know and what you don't know. If you are struggling, study some more, review, and then assess your knowledge again.
- **Review the objectives**—Develop your own questions and examples for each objective listed. If you can develop and answer several questions for each objective, you should not find it difficult to pass the exam.

NOTE

Exam-Taking Advice Although this book is designed to prepare you to take and pass the CISA exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exam and additional exams provided in the MeasureUp test software. Your results should tell you whether you are ready for the real thing.

When taking the actual certification exam, make sure you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best as you can; then mark it for review when you have finished the rest of the questions.

Remember that the primary goal is not just to pass the exam, but to understand the material. When you understand the material, passing the exam will be much easier. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the CISA certification are designed to help you build your IT audit and IT security future.

Good luck!