

David L. Cannon

CISA[®]

**Certified Information
Systems Auditor**

STUDY GUIDE

Fourth Edition

Covers 100% of CISA's most current objectives including, IT Governance, The IS Audit Process, System Implementation and Operations, Protecting Information Assets and much more...

Includes interactive online learning environment with:

- + **Hundreds of sample questions**
- + **Electronic flashcards**
- + **Searchable key term glossary**
- + **Instructional video**
- + **Interactive test engine**



SYBEX
A Wiley Brand

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

Copyright © 2016 by John Wiley & Sons, Inc., Indianapolis, Indiana

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

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2015960605

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CISA is a registered trademark of Information Systems Audit and Control Association, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

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

<i>Introduction</i>		<i>xix</i>
<i>Assessment Test</i>		<i>xlii</i>
Chapter 1	Secrets of a Successful Auditor	1
Chapter 2	Governance	57
Chapter 3	Audit Process	139
Chapter 4	Networking Technology Basics	215
Chapter 5	Information Systems Life Cycle	307
Chapter 6	System Implementation and Operations	381
Chapter 7	Protecting Information Assets	449
Chapter 8	Business Continuity and Disaster Recovery	517
Appendix	Answers to Review Questions	571
<i>Index</i>		<i>591</i>

Contents

<i>Introduction</i>	<i>xix</i>	
<i>Assessment Test</i>	<i>xlii</i>	
Chapter 1	Secrets of a Successful Auditor	1
Understanding the Demand for IS Audits		2
Executive Misconduct		3
More Regulation Ahead		5
Basic Regulatory Objective		7
Governance Is Leadership		8
Three Types of Data Target Different Uses		9
Audit Results Indicate the Truth		10
Understanding Policies, Standards, Guidelines, and Procedures		11
Understanding Professional Ethics		14
Following the ISACA Professional Code		14
Preventing Ethical Conflicts		16
Understanding the Purpose of an Audit		17
Classifying General Types of Audits		18
Determining Differences in Audit Approach		20
Understanding the Auditor's Responsibility		21
Comparing Audits to Assessments		21
Differentiating between Auditor and Auditee Roles		22
Applying an Independence Test		23
Implementing Audit Standards		24
Where Do Audit Standards Come From?		25
Understanding the Various Auditing Standards		27
Specific Regulations Defining Best Practices		31
Audits to Prove Financial Integrity		34
Auditor Is an Executive Position		35
Understanding the Importance of Auditor Confidentiality		35
Working with Lawyers		36
Working with Executives		37
Working with IT Professionals		37
Retaining Audit Documentation		38
Providing Good Communication and Integration		39
Understanding Leadership Duties		39
Planning and Setting Priorities		40
Providing Standard Terms of Reference		41
Dealing with Conflicts and Failures		42

Identifying the Value of Internal and External Auditors	43
Understanding the Evidence Rule	43
Stakeholders: Identifying Whom You Need to Interview	44
Understanding the Corporate Organizational Structure	45
Identifying Roles in a Corporate Organizational Structure	45
Identifying Roles in a Consulting Firm Organizational Structure	47
Summary	49
Exam Essentials	49
Review Questions	52
Chapter 2	Governance
	57
Strategy Planning for Organizational Control	61
Overview of the IT Steering Committee	64
Using the Balanced Scorecard	69
IT Subset of the BSC	74
Decoding the IT Strategy	74
Specifying a Policy	77
Project Management	79
Implementation Planning of the IT Strategy	90
Using COBIT	94
Identifying Sourcing Locations	94
Conducting an Executive Performance Review	99
Understanding the Auditor's Interest in the Strategy	100
Overview of Tactical Management	100
Planning and Performance	100
Management Control Methods	101
Risk Management	105
Implementing Standards	108
Human Resources	109
System Life-Cycle Management	111
Continuity Planning	111
Insurance	112
Overview of Business Process Reengineering	112
Why Use Business Process Reengineering	113
BPR Methodology	114
Genius or Insanity?	114
Goal of BPR	114
Guiding Principles for BPR	115
Knowledge Requirements for BPR	116
BPR Techniques	116

BPR Application Steps	117
Role of IS in BPR	119
Business Process Documentation	119
BPR Data Management Techniques	120
Benchmarking as a BPR Tool	120
Using a Business Impact Analysis	121
BPR Project Risk Assessment	123
Practical Application of BPR	125
Practical Selection Methods for BPR	127
Troubleshooting BPR Problems	128
Understanding the Auditor’s Interest in Tactical Management	129
Operations Management	129
Sustaining Operations	130
Tracking Actual Performance	130
Controlling Change	131
Understanding the Auditor’s Interest in Operational Delivery	131
Summary	132
Exam Essentials	132
Review Questions	134

Chapter 3 Audit Process 139

Understanding the Audit Program	140
Audit Program Objectives and Scope	141
Audit Program Extent	143
Audit Program Responsibilities	144
Audit Program Resources	144
Audit Program Procedures	145
Audit Program Implementation	146
Audit Program Records	146
Audit Program Monitoring and Review	147
Planning Individual Audits	148
Establishing and Approving an Audit Charter	151
Role of the Audit Committee	151
Preplanning Specific Audits	153
Understanding the Variety of Audits	154
Identifying Restrictions on Scope	156
Gathering Detailed Audit Requirements	158
Using a Systematic Approach to Planning	159
Comparing Traditional Audits to Assessments and Self-Assessments	161
Performing an Audit Risk Assessment	162

Determining Whether an Audit Is Possible	163
Identifying the Risk Management Strategy	165
Determining Feasibility of Audit	167
Performing the Audit	167
Selecting the Audit Team	167
Determining Competence and Evaluating Auditors	168
Ensuring Audit Quality Control	170
Establishing Contact with the Auditee	171
Making Initial Contact with the Auditee	172
Using Data Collection Techniques	174
Conducting Document Review	176
Understanding the Hierarchy of Internal Controls	177
Reviewing Existing Controls	179
Preparing the Audit Plan	182
Assigning Work to the Audit Team	183
Preparing Working Documents	184
Conducting Onsite Audit Activities	185
Gathering Audit Evidence	186
Using Evidence to Prove a Point	186
Understanding Types of Evidence	187
Selecting Audit Samples	187
Recognizing Typical Evidence for IS Audits	188
Using Computer-Assisted Audit Tools	189
Understanding Electronic Discovery	191
Grading of Evidence	193
Timing of Evidence	195
Following the Evidence Life Cycle	195
Conducting Audit Evidence Testing	198
Compliance Testing	198
Substantive Testing	199
Tolerable Error Rate	200
Recording Test Results	200
Generating Audit Findings	201
Detecting Irregularities and Illegal Acts	201
Indicators of Illegal or Irregular Activity	202
Responding to Irregular or Illegal Activity	202
Findings Outside of Audit Scope	203
Report Findings	203
Approving and Distributing the Audit Report	205
Identifying Omitted Procedures	205
Conducting Follow-up (Closing Meeting)	205
Summary	206
Exam Essentials	207
Review Questions	210

Chapter 4	Networking Technology Basics	215
	Understanding the Differences in Computer Architecture	217
	Selecting the Best System	221
	Identifying Various Operating Systems	221
	Determining the Best Computer Class	224
	Comparing Computer Capabilities	227
	Ensuring System Control	228
	Dealing with Data Storage	230
	Using Interfaces and Ports	235
	Introducing the Open Systems Interconnection Model	237
	Layer 1: Physical Layer	240
	Layer 2: Data-Link Layer	240
	Layer 3: Network Layer	242
	Layer 4: Transport Layer	248
	Layer 5: Session Layer	249
	Layer 6: Presentation Layer	250
	Layer 7: Application Layer	250
	Understanding How Computers Communicate	251
	Understanding Physical Network Design	252
	Understanding Network Cable Topologies	253
	Bus Topologies	254
	Star Topologies	254
	Ring Topologies	255
	Meshed Networks	256
	Differentiating Network Cable Types	258
	Coaxial Cable	258
	Unshielded Twisted-Pair (UTP) Cable	259
	Fiber-Optic Cable	260
	Connecting Network Devices	260
	Using Network Services	263
	Domain Name System	263
	Dynamic Host Configuration Protocol	265
	Expanding the Network	266
	Using Telephone Circuits	268
	Network Firewalls	271
	Remote VPN Access	276
	Using Wireless Access Solutions	280
	Firewall Protection for Wireless Networks	284
	Remote Dial-Up Access	284
	WLAN Transmission Security	284
	Achieving 802.11i RSN Wireless Security	287
	Intrusion Detection Systems	288
	Summarizing the Various Area Networks	291

	Using Software as a Service (SaaS)	292
	Advantages	292
	Disadvantages	293
	Cloud Computing	294
	The Basics of Managing the Network	295
	Automated LAN Cable Tester	295
	Protocol Analyzers	295
	Remote Monitoring Protocol Version 2	297
	Summary	298
	Exam Essentials	298
	Review Questions	301
Chapter 5	Information Systems Life Cycle	307
	Governance in Software Development	308
	Management of Software Quality	310
	Capability Maturity Model	310
	International Organization for Standardization	312
	Typical Commercial Records Classification Method	316
	Overview of the Executive Steering Committee	317
	Identifying Critical Success Factors	318
	Using the Scenario Approach	318
	Aligning Software to Business Needs	319
	Change Management	323
	Management of the Software Project	323
	Choosing an Approach	323
	Using Traditional Project Management	324
	Overview of the System Development Life Cycle	327
	Phase 1: Feasibility Study	331
	Phase 2: Requirements Definition	334
	Phase 3: System Design	339
	Phase 4: Development	343
	Phase 5: Implementation	354
	Phase 6: Postimplementation	361
	Phase 7: Disposal	363
	Overview of Data Architecture	364
	Databases	364
	Database Transaction Integrity	368
	Decision Support Systems	369
	Presenting Decision Support Data	370
	Using Artificial Intelligence	370
	Program Architecture	371
	Centralization vs. Decentralization	372
	Electronic Commerce	372

Summary	374
Exam Essentials	374
Review Questions	376
Chapter 6	System Implementation and Operations
	381
Understanding the Nature of IT Services	383
Performing IT Operations Management	385
Meeting IT Functional Objectives	385
Using the IT Infrastructure Library	387
Supporting IT Goals	389
Understanding Personnel Roles and Responsibilities	389
Using Metrics	394
Evaluating the Help Desk	396
Performing Service-Level Management	397
Outsourcing IT Functions	398
Performing Capacity Management	399
Using Administrative Protection	400
Information Security Management	401
IT Security Governance	401
Authority Roles over Data	402
Data Retention Requirements	403
Document Physical Access Paths	404
Personnel Management	405
Physical Asset Management	406
Compensating Controls	408
Performing Problem Management	409
Incident Handling	410
Digital Forensics	412
Monitoring the Status of Controls	414
System Monitoring	415
Document Logical Access Paths	416
System Access Controls	417
Data File Controls	420
Application Processing Controls	421
Log Management	423
Antivirus Software	424
Active Content and Mobile Software Code	424
Maintenance Controls	427
Implementing Physical Protection	430
Data Processing Locations	432
Environmental Controls	432
Safe Media Storage	440

	Summary	442
	Exam Essentials	442
	Review Questions	444
Chapter 7	Protecting Information Assets	449
	Understanding the Threat	450
	Recognizing Types of Threats and Computer Crimes	452
	Identifying the Perpetrators	454
	Understanding Attack Methods	458
	Implementing Administrative Protection	469
	Using Technical Protection	472
	Technical Control Classification	472
	Application Software Controls	474
	Authentication Methods	475
	Network Access Protection	488
	Encryption Methods	489
	Public-Key Infrastructure	496
	Network Security Protocols	502
	Telephone Security	507
	Technical Security Testing	507
	Summary	509
	Exam Essentials	509
	Review Questions	511
Chapter 8	Business Continuity and Disaster Recovery	517
	Debunking the Myths	518
	Myth 1: Facility Matters	519
	Myth 2: IT Systems Matter	519
	From Myth to Reality	519
	Understanding the Five Conflicting Disciplines	
	Called Business Continuity	520
	Defining Disaster Recovery	521
	Surviving Financial Challenges	522
	Valuing Brand Names	522
	Rebuilding after a Disaster	523
	Defining the Purpose of Business Continuity	524
	Uniting Other Plans with Business Continuity	527
	Identifying Business Continuity Practices	527
	Identifying the Management Approach	529
	Following a Program Management Approach	531

Understanding the Five Phases of a Business	
Continuity Program	532
Phase 1: Setting Up the BC Program	532
Phase 2: The Discovery Process	535
Phase 4: Plan Implementation	560
Phase 5: Maintenance and Integration	562
Understanding the Auditor Interests in BC/DR Plans	563
Summary	564
Exam Essentials	564
Review Questions	566
Appendix	Answers to Review Questions
	571
<i>Index</i>	591

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