



# CISA<sup>®</sup>

Certified Information  
Systems Auditor

# STUDY GUIDE

**COVERS 2024-2029 EXAM OBJECTIVES**

Includes interactive online learning environment and study tools:

**2 custom practice exams**

**100 electronic flashcards**

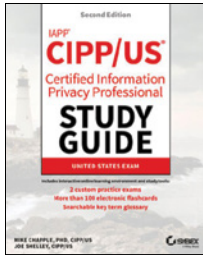
**Searchable key term glossary**

PETER H. GREGORY, CISA, CISSP  
MIKE CHAPPLE, PH.D., CISA, CISSP

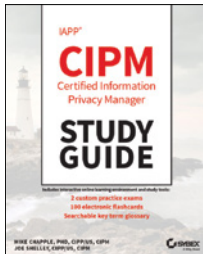
 **SYBEX<sup>®</sup>**  
A Wiley Brand



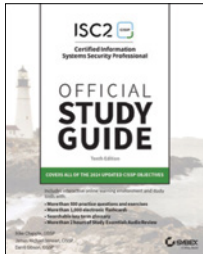
## Other Information Security Study Guides from Sybex



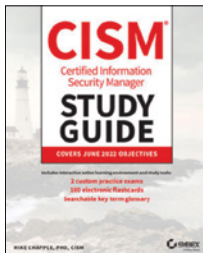
IAPP CIPP / US Certified Information Privacy Professional Study Guide, 2nd Edition — ISBN 978-1-394-28490-0, January 2025



IAPP CIPM Certified Information Privacy Manager Study Guide — ISBN 978-1-394-15380-0, January 2023



ISC2 CISSP Certified Information Systems Security Professional Official Study Guide, 10th Edition — ISBN 978-1-394-25469-9, June 2024



CISM Certified Information Security Manager Study Guide — ISBN 978-1-119-80193-1, May 2022



ISC2 CCSP Certified Cloud Security Professional Official Study Guide, 3rd Edition — ISBN 978-1-119-90937-8, October 2022



# **CISA®**

# **Certified Information Systems Auditor**

## **Study Guide**

**Covers 2024–2029 Exam Objectives**



Peter H. Gregory, CISA, CISSP  
Mike Chapple, Ph.D., CISA, CISSP



Copyright © 2025 by John Wiley & Sons, Inc. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

Some content was previously published in CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition by Peter H. Gregory (© 2020 McGraw-Hill).

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394288380 (paperback), 9781394288403 (ePDF), 9781394288397 (ePub)

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). 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 [www.wiley.com/go/permission](http://www.wiley.com/go/permission).

**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 trademark or 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.

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

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

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

**Library of Congress Control Number:** 2024942279

Cover image: © Jeremy Woodhouse/Getty Images

Cover design: Wiley

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

*—Peter*

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

*—Mike*

# Acknowledgments

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

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

Shahla Pirnia, Mike's technical editor at CertMike.com, was instrumental in helping us get all of the details straightened out as we prepared the manuscript.

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

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



# About the Authors

**Peter H. Gregory, CISSP, CISM, CISA, CRISC, CIPM, CDPSE, CCSK, DRCE, A/CCRF, A/CCRP**, is the author of more than 60 books on security and technology, including *Solaris Security* (Prentice Hall, 2000), *The Art of Writing Technical Books* (Waterside Productions, 2022), *CISM Certified Information Security Manager All-In-One Exam Guide* (McGraw-Hill, 2022), *Chromebook For Dummies* (Wiley, 2023), and *Elementary Information Security* (Jones & Bartlett Learning, 2024).

Peter is a career technologist and a security executive at a regional telecommunications provider. Before this, he held security leadership positions at Optiv Security ([www.optiv.com](http://www.optiv.com)) and Concur Technologies ([www.concur.com](http://www.concur.com)). Peter is an advisory board member for the University of Washington and Seattle University for education programs in cybersecurity. He is a graduate of the FBI Citizens Academy.

Peter resides in Central Washington State and can be found at [www.peterhgregory.com](http://www.peterhgregory.com).

**Mike Chapple, PhD, CISA**, is the author of over 50 books, including the best-selling *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide* (Sybex, 2024) and the *ISC2 CISSP Official Practice Tests* (Sybex, 2024). He is a cybersecurity professional with 25 years of experience in higher education, the private sector, and government.

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

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

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering. Mike also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the Certified Information Systems Auditor (CISA), Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

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

# About the Technical Editors

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

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

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

# Contents at a Glance

<i>Introduction</i>	<i>xxiii</i>
<i>Assessment Test</i>	<i>xxxv</i>
<b>Chapter 1</b>	IT Governance and Management 1
<b>Chapter 2</b>	The Audit Process 87
<b>Chapter 3</b>	IT Life Cycle Management 157
<b>Chapter 4</b>	IT Service Management 271
<b>Chapter 5</b>	IT Infrastructure 309
<b>Chapter 6</b>	Business Continuity and Disaster Recovery 405
<b>Chapter 7</b>	Information Security Management 491
<b>Chapter 8</b>	Identity and Access Management 567
<b>Chapter 9</b>	Conducting a Professional Audit 623
<b>Appendix A</b>	Popular Methodologies, Frameworks, and Guidance 701
<b>Appendix B</b>	Answers to Review Questions 741
<i>Index</i>	<i>759</i>



# Contents

*Introduction* *xxiii*

*Assessment Test* *xxxv*

<b>Chapter 1</b>	<b>IT Governance and Management</b>	<b>1</b>
	IT Governance Practices for Executives and Boards of Directors	3
	IT Governance	4
	IT Governance Frameworks	4
	IT Strategy Committee	6
	The Balanced Scorecard	6
	Information Security Governance	7
	IT Strategic Planning	10
	The IT Steering Committee	11
	Policies, Processes, Procedures, and Standards	12
	Information Security Policy	14
	Privacy Policy	14
	Data Classification Policy	15
	System Classification Policy	16
	Site Classification Policy	16
	Access Control Policy	16
	Mobile Device Policy	16
	Social Media Policy	17
	Other Policies	17
	Processes and Procedures	17
	Standards	18
	Enterprise Architecture	20
	Applicable Laws, Regulations, and Standards	23
	Risk Management	23
	The Risk Management Program	25
	The Risk Management Process	25
	Risk Treatment	36
	IT Management Practices	39
	Personnel Management	40
	Sourcing	46
	Change Management	55
	Financial Management	55
	Quality Management	56
	Portfolio Management	58
	Controls Management	59
	Security Management	60

Performance and Capacity Management	61
Organization Structure and Responsibilities	62
Roles and Responsibilities	64
Segregation of Duties	71
Maintaining an Existing Program	72
Metrics and Monitoring	74
Reporting	75
Auditing IT Governance	75
Auditing Documentation and Records	76
Auditing Contracts	78
Auditing Outsourcing	79
Summary	80
Exam Essentials	81
Review Questions	83
<b>Chapter 2    The Audit Process</b>	<b>87</b>
Audit Management	89
The Audit Charter	89
The Audit Program	90
Strategic Audit Planning	90
Audit and Technology	93
Audit Laws and Regulations	94
ISACA Auditing Standards	99
ISACA Code of Professional Ethics	100
ISACA Audit and Assurance Standards	100
ISACA Audit and Assurance Guidelines	103
Risk Analysis	108
Auditors' Risk Analysis and the Corporate	
Risk Management Program	109
Evaluating Business Processes	111
Identifying Business Risks	112
Risk Mitigation	113
Countermeasures Assessment	114
Monitoring	114
Using AI and ML in Support of Audits	114
Controls	115
Control Classification	115
Internal Control Objectives	118
IS Control Objectives	119
General Computing Controls	120
IS Controls	120
Performing an Audit	121
Audit Objectives	122
Types of Audits	123

Compliance vs. Substantive Testing	125
Audit Methodology and Project Management	125
Audit Evidence	129
Agile Auditing	135
Reliance on the Work of Other Auditors	135
Audit Data Analytics	136
Reporting Audit Results	139
Other Audit Topics	141
Control Self-Assessment	144
CSA Advantages and Disadvantages	145
The CSA Life Cycle	145
Self-Assessment Objectives	146
Auditors and Self-Assessment	147
Implementation of Audit Recommendations	147
Audit Quality Assurance	148
Summary	148
Exam Essentials	150
Review Questions	152
<b>Chapter 3 IT Life Cycle Management</b>	<b>157</b>
Benefits Realization	159
Portfolio and Program Governance and Management	160
Business Case and Feasibility Analysis Development	163
Measuring Business Benefits	164
Project Management	165
Organizing Projects	165
Developing Project Objectives	167
Managing Projects	169
Project Roles and Responsibilities	170
Project Planning	171
Project Management Methodologies	185
Systems Development Methodologies	191
SDLC Methodology Phases	192
Software Development Risks	221
Alternative Software Development Approaches and Techniques	222
System Development Tools	226
Acquiring Cloud-Based Infrastructure and Applications	228
Infrastructure Development and Deployment	230
Review of Existing Architecture	230
Requirements	231
Design	232
Procurement	232
Testing	233

Implementation	234
Maintenance	234
Maintaining Information Systems	234
Change Management	234
Configuration Management	236
Business Processes	237
The Business Process Life Cycle and Business Process	
Reengineering	237
Capability Maturity Models	240
Managing Third Parties	244
Risk Factors	244
Onboarding and Due Diligence	245
Classification	245
Assessment	246
Remediation	246
Risk Reporting	246
Application Controls	247
Input Controls	247
Processing Controls	250
Output Controls	252
Auditing the Systems Development Life Cycle	253
Auditing Program and Project Management	253
Auditing the Feasibility Study	254
Auditing Requirements	254
Auditing Design	255
Auditing Software Acquisition	255
Auditing Development	255
Auditing Testing	256
Auditing Implementation	256
Auditing Post-Implementation	257
Auditing Change Management	257
Auditing Configuration Management	257
Auditing Business Controls	258
Auditing Application Controls	258
Transaction Flow	258
Observations	259
Data Integrity Testing	259
Testing Online Processing Systems	259
Auditing Applications	260
Continuous Auditing	261
Auditing Third-Party Risk Management	261
Summary	262
Exam Essentials	264
Review Questions	266



<b>Chapter 4</b>	<b>IT Service Management</b>	<b>271</b>
	Information Systems Operations	273
	Management and Control of Operations	274
	Systems Performance Management	274
	Availability Management	274
	Capacity Management	275
	System and Security Monitoring	276
	Problem and Incident Management	277
	Change, Configuration, Release, and Patch Management	279
	Change Management	279
	Configuration Management	281
	Release Management	282
	Patch Management	285
	Operational Log Management	286
	Types of Log Entries	286
	Log Management	287
	IT Operations and Exception Handling	287
	IT Service Level Management	288
	Database Management Systems	290
	DBMS Organization	290
	Managing a DBMS	290
	DBMS Structure	290
	Data Management and Governance	294
	Data Life Cycle	294
	Data Quality Management	295
	Other IT Service Management Topics	295
	Financial Management	295
	Quality Assurance	296
	Security Management	296
	Media Control	296
	Auditing IT Service Management and Operations	297
	Auditing Computer Operations	297
	Auditing File Management	298
	Auditing Data Entry	298
	Auditing Lights-Out Operations	299
	Auditing Problem Management Operations	299
	Auditing Monitoring Operations	299
	Auditing Procurement	300
	Auditing Database Management Systems	300
	Summary	301
	Exam Essentials	302
	Review Questions	304

<b>Chapter 5</b>	<b>IT Infrastructure</b>	<b>309</b>
	Information Systems Hardware	310
	Computer Usage	310
	Multicomputer Architectures	320
	Hardware Maintenance	322
	Hardware Monitoring	323
	Information Systems Architecture and Software	324
	Computer Operating Systems	324
	Data Communications Software	325
	Filesystems	326
	Media Management Systems	327
	Utility Software	327
	Software Licensing	328
	Digital Rights Management	329
	Network Infrastructure	330
	Enterprise Architecture	330
	Network Architecture	331
	Network-Based Services	333
	Network Models	336
	Network Technologies	346
	Asset Inventory and Classification	386
	Hardware Asset Inventory	387
	Information Assets	388
	Job Scheduling and Production Process Automation	390
	System Interfaces	391
	End-User Computing	392
	Shadow IT	393
	Auditing IT Infrastructure	393
	Auditing Information Systems Hardware	394
	Auditing Operating Systems	394
	Auditing Filesystems	395
	Auditing Database Management Systems	395
	Auditing Network Infrastructure	396
	Auditing Network Operating Controls	397
	Auditing IT Operations	397
	Summary	398
	Exam Essentials	399
	Review Questions	401
<b>Chapter 6</b>	<b>Business Continuity and Disaster Recovery</b>	<b>405</b>
	Business Resilience	406
	Business Continuity Planning	406
	Disaster Recovery Planning	449

Incident Response Communications	473
Crisis Management and Communications	473
Communications in the Incident Response Plan	474
Auditing Business Continuity Planning	475
Auditing Business Continuity Documentation	476
Reviewing Prior Test Results and Action Plans	477
Interviewing Key Personnel	478
Reviewing Service Provider Contracts	478
Reviewing Insurance Coverage	479
Visiting Media Storage and Alternate Processing Sites	479
Auditing Disaster Recovery Planning	479
Auditing Disaster Recovery Plans	480
Reviewing Prior DR Test Results and Action Plans	481
Evaluating Off-site Storage	482
Evaluating Alternate Processing Facilities	483
Summary	484
Exam Essentials	485
Review Questions	487
<b>Chapter 7</b>	<b>Information Security Management 491</b>
Information Security	493
Role of the Information Security Manager	494
Chief Information Security Officer	495
Lines of Authority	495
Organizing the Security Team	496
Roles and Responsibilities	496
Information Security Risks	497
The DAD Triad	498
Incident Impact	499
Building an Information Security Strategy	501
Threat Research	501
SWOT Analysis	502
Gap Analysis	502
Alignment with Business Strategy	503
Cybersecurity Responsibilities	504
Implementing Security Controls	505
Security Control Categories	505
Security Control Types	506
Endpoint Security	507
Malware Prevention	507
Endpoint Detection and Response	507
Data Loss Prevention	508
Change and Configuration Management	509
Patch Management	509

System Hardening	510
Mobile, Wireless, and Internet of Things Devices	510
Network Security Controls	511
Network Segmentation	511
Network Device Security	513
Network Security Tools	515
Cloud Computing Security	519
Benefits of the Cloud	520
Cloud Roles	522
Cloud Service Models	522
Cloud Deployment Models	523
Shared Responsibility Model	524
Cloud Security Issues	525
Cloud Security Controls	527
Cryptography	528
Goals of Cryptography	529
Symmetric Key Algorithms	531
Asymmetric Cryptography	532
Hash Functions	533
Digital Signatures	534
Digital Certificates	535
Certificate Management	536
Exploring Cybersecurity Threats	539
Classifying Cybersecurity Threats	539
Threat Actors	540
Threat Vectors	543
Privacy	545
Sensitive Information Inventory	545
Data Classification	546
Information Life Cycle	547
Privacy and Data Breach Notification	547
Security Awareness and Training	548
User Training	548
Role-Based Training	548
Ongoing Awareness Efforts	549
Security Incident Response	550
Phases of Incident Response	550
Evidence Collection and Forensics	552
Auditing Information Security Controls	554
Auditing Security Management	554
Auditing Network Security Controls	555
Summary	559
Exam Essentials	560
Review Questions	563

<b>Chapter 8</b>	<b>Identity and Access Management</b>	<b>567</b>
	Logical Access Controls	568
	Access Control Concepts	569
	Access Control Models	569
	Access Control Threats	570
	Access Control Vulnerabilities	571
	Access Points and Methods of Entry	573
	Identification, Authentication, and Authorization	576
	Authentication Techniques	577
	Authentication Errors	579
	Single Sign-on and Federation	580
	Provisioning and Deprovisioning	580
	Account Monitoring	581
	Access Control Lists	582
	Protecting Stored Information	582
	Third-party Access Management	587
	Third Parties and Risk	587
	Types of Third-Party Access	588
	Risks Associated with Third-Party Access	588
	Third-Party Access Countermeasures	588
	Third-Party Security in Legal Agreements	590
	Third-Party Security in Security Policy	590
	Third-Party Risk Management Life Cycle	591
	Environmental Controls	592
	Environmental Threats and Vulnerabilities	592
	Environmental Controls and Countermeasures	593
	Physical Security Controls	599
	Physical Access Threats and Vulnerabilities	599
	Physical Access Controls and Countermeasures	601
	Human Resources Security	602
	Screening and Background Checks	603
	Job Descriptions	604
	Employment Agreements	604
	Personnel Security Controls	605
	Transfers and Terminations	606
	Auditing Access Controls	606
	Auditing Logical Access Controls	606
	Auditing Environmental Controls	614
	Auditing Physical Security Controls	615
	Summary	616
	Exam Essentials	617
	Review Questions	619

<b>Chapter 9</b>	<b>Conducting a Professional Audit</b>	<b>623</b>
	Understanding the Audit Cycle	624
	How the IS Audit Cycle Is Discussed	625
	“Client” and Other Terms in This Chapter	626
	Overview of the IS Audit Cycle	627
	Project Origination	628
	Engagement Letters and Audit Charters	636
	Ethics and Independence	640
	Launching a New Project: Planning an Audit	641
	Developing the Audit Plan	645
	Developing a Test Plan	649
	Performing a Pre-Audit (or Readiness Assessment)	657
	Organizing a Testing Plan	660
	Resource Planning for the Audit Team	663
	Developing Audit Opinions	683
	Developing Audit Recommendations	685
	Managing Supporting Documentation	685
	Delivering Audit Results	687
	Management Response	692
	Audit Closing Procedures	697
	Audit Follow-up	698
	Summary	699
<b>Appendix A</b>	<b>Popular Methodologies, Frameworks, and Guidance</b>	<b>701</b>
	Common Terms and Concepts	702
	Governance	703
	Goals, Objectives, and Strategies	703
	Processes	704
	Capability Maturity Models	705
	Controls	707
	The Deming Cycle	708
	Projects	709
	Frameworks, Methodologies, and Guidance	710
	Business Model for Information Security (BMIS)	710
	COSO Internal Control – Integrated Framework	711
	COBIT	715
	GTAG	717
	ISF Standard of Good Practice for Information Security	717
	ISO/IEC 27001 and 27002	718
	NIST SP 800-53 and NIST SP 800-53A	719
	NIST Cybersecurity Framework	720
	Payment Card Industry Data Security Standard (PCI DSS)	722
	CIS Critical Security Controls	725

	IT Assurance Framework	726
	ITIL	728
	PMBOK® Guide	729
	PRINCE2	731
	Risk IT	732
	Summary of Frameworks	733
	Pointers for Successful Use of Frameworks	738
	Notes	738
	References	738
<b>Appendix B</b>	<b>Answers to Review Questions</b>	<b>741</b>
	Chapter 1: IT Governance and Management	742
	Chapter 2: The Audit Process	744
	Chapter 3: IT Life Cycle Management	746
	Chapter 4: IT Service Management	748
	Chapter 5: IT Infrastructure	749
	Chapter 6: Business Continuity and Disaster Recovery	750
	Chapter 7: Information Security Management	752
	Chapter 8: Identity and Access Management	754
<i>Index</i>		759





# Introduction

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

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

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

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

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

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

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

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

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

This book presents the material at an intermediate technical level. Experience with and knowledge of security and auditing concepts will help you get a full understanding of the challenges you'll face as an information systems auditor.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. We recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam.

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



---

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

## The CISA Exam

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

The exam covers five major domains:

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

These five areas include a range of topics, from enterprise risk management to evaluating cybersecurity controls. They focus heavily on scenario-based learning and the role of the information systems auditor in various scenarios. There's a lot of information that you'll need to learn, but you'll be well rewarded for possessing this credential. ISACA reports that the average salary of CISA credential holders is over \$145,000.

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

The exam costs \$575 for ISACA members and \$760 for non-members. More details about the CISA exam and how to take it can be found at:

[www.isaca.org/credentialing/cisa](http://www.isaca.org/credentialing/cisa)

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



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

## Taking the Exam

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

### In-Person Exams

ISACA partners with PSI Exams testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your zip code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the PSI Exams website:

<https://home.psiexams.com/#/test-center?p=Z97SE74H>

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

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

## **At-Home Exams**

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

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

## **After the CISA Exam**

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

## **Meeting the Experience Requirement**

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

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

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

There are some waivers available that can knock 1, 2, or 3 years off your experience requirement:

- If you hold an associate's degree in any field, you qualify for a 1-year waiver.
- If you hold a bachelor's, master's, or doctoral degree in any field, you qualify for a 2-year waiver.
- If you hold a master's degree in information systems or a related field, you qualify for a 3-year waiver.
- If you hold full certification from the Chartered Institute of Management Accountants (CIMA), you qualify for a 2-year waiver.
- If you are a member of the Association of Chartered Certified Accountants (ACCA), you qualify for a 2-year waiver.



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

You must have earned all of the experience used toward your requirement within the 10 years preceding your application or within 5 years of the date you pass the exam.

## Maintaining Your Certification

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

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

You must meet both of these requirements. For example, if you earn 120 credit hours during the first year of your certification cycle, you still must earn 20 additional credits in each of the next 2 years.

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

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

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

For more information on the activities that qualify for CPE credits, visit this site:

[www.isaca.org/credentialing/how-to-earn-cpe](http://www.isaca.org/credentialing/how-to-earn-cpe)

## Study Guide Elements

This study guide uses a number of common elements to help you prepare. These include the following:

**Summaries** The Summary section of each chapter briefly explains the chapter, allowing you to easily understand what it covers.

**Exam Essentials** The Exam Essentials focus on major exam topics and critical knowledge that you should take in to the test. The Exam Essentials focus on the exam objectives provided by ISACA.

**Chapter Review Questions** A set of questions at the end of each chapter will help you assess your knowledge and if you are ready to take the exam based on your knowledge of that chapter's topics.

## Additional Study Tools

This book comes with a number of additional study tools to help you prepare for the exam. They include the following.



Go to [www.wiley.com/go/Sybextestprep](http://www.wiley.com/go/Sybextestprep) to register and gain access to this interactive online learning environment and test bank with study tools.

## Sybex Test Preparation Software

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

## Electronic Flashcards

Our electronic flashcards are designed to help you prepare for the exam. Over 100 flashcards will ensure that you know critical terms and concepts.

## Glossary of Terms

Sybex provides a full glossary of terms in PDF format, allowing quick searches and easy reference to materials in this book.

## Bonus Practice Exams

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