

# **CISA<sup>®</sup>: Certified Information Systems Auditor**

**Study Guide  
Fourth Edition**



# **CISA<sup>®</sup>: Certified Information Systems Auditor**

**Study Guide  
Fourth Edition**



David Cannon

with Brian T. O'Hara and Allen Keele

 **SYBEX<sup>®</sup>**  
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](http://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](http://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](mailto: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>
<b>Chapter 1</b>	Secrets of a Successful Auditor	1
<b>Chapter 2</b>	Governance	57
<b>Chapter 3</b>	Audit Process	139
<b>Chapter 4</b>	Networking Technology Basics	215
<b>Chapter 5</b>	Information Systems Life Cycle	307
<b>Chapter 6</b>	System Implementation and Operations	381
<b>Chapter 7</b>	Protecting Information Assets	449
<b>Chapter 8</b>	Business Continuity and Disaster Recovery	517
<b>Appendix</b>	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>	
<b>Chapter 1</b>	<b>Secrets of a Successful Auditor</b>	<b>1</b>
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
<b>Chapter 2</b>	<b>Governance</b>
	<b>57</b>
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