

# **CISA<sup>®</sup>**

# **Certified Information Systems Auditor<sup>™</sup>**

**Study Guide**

**Second Edition**



David L. Cannon



Wiley Publishing, Inc.



**CISA®**  
**Certified Information**  
**Systems Auditor™**  
**Study Guide**  
**Second Edition**







# **CISA<sup>®</sup>**

# **Certified Information Systems Auditor<sup>™</sup>**

**Study Guide**

**Second Edition**



David L. Cannon



Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum  
Development Editor: Lisa Bishop  
Technical Editor: Brady Pamplin  
Production Editor: Rachel McConlogue  
Copy Editor: Sharon Wilkey  
Production Manager: Tim Tate  
Vice President and Executive Group Publisher: Richard Swadley  
Vice President and Executive Publisher: Joseph B. Wikert  
Vice President and Publisher: Neil Edde  
Media Project Manager: Laura Atkinson  
Media Assistant Producer: Angie Denny  
Media Quality Assurance: Josh Frank  
Book Designer: Judy Fung and Bill Gibson  
Compositor: Craig Woods, Happenstance Type-O-Rama  
Proofreader: Jen Larsen, Word One  
Indexer: Ted Laux  
Cover Designer: Ryan Sneed

Copyright © 2008 by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-23152-4

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 Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, 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 Website 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 Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites 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 (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data is available from the publisher.

**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 and Certified Information Systems Auditor are trademarks or registered trademarks of Information Systems Audit and Control Association. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1



Dear Reader,

Thank you for choosing *CISA: Certified Information Systems Auditor*. This book is part of a family of premium quality Sybex books, all written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than thirty years later, we're still committed to producing consistently exceptional books. With each of our titles we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at [nedde@wiley.com](mailto:nedde@wiley.com), or if you think you've found a technical error in this book, please visit <http://sybex.custhelp.com>. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde  
Vice President & Publisher  
Wiley Publishing, Inc.

*This book is a tribute to the students who attended our classes. Their infinite questions were instrumental in the creation of this Study Guide. I wish to express my appreciation to my past employers and clients for the opportunities that led me down this path.*

*I would like to express a special appreciation to the following people for their years of encouragement: Kristine Lindamood, Carl Adkins, Thomas Carson Jr., Jeff Kellum, Reno Marsh, Toni Spray, Dewayne Neagle, Scott Barber, Richard Darrell, William “Bill” Giles, Tim and Cynthia McDonald, Pat Cathey, Lori Martin, Gary Sprague, Lori Acree, Terry Perkins, Mike English, Sean Burke, Mike Pratt, Dianna Pickens, David Bassham, Timothy S. Bergmann, Brady Pamplin, Mark and Kris Herber, Wendy Stevens, Brian Wrozek, Frank Carter, Kris Lonborg, Joe Moore, Danney Jarmon, Bob Mahlstedt, Chris and Tammy Stevens, Daryl Luthas, Stephen Harding, Kirk Pingel, Darlene Miller, Matt Gair, Nan Robinson, Tarik Nasir, Gary and Michelle Ames, Mitch and Cindy Waters.*

*I thank my family—Del, Martha, Rose Ann, John, Joann, and my grandmother Josephine—for their support. In addition, I have been blessed to work with the best staff on this planet: Joe DeVoss, Melissa Robinson, Tom Kormondy, Kayla McGee, Alan Yue, Jon Murphy, and Steve Lineberry.*

*Semper Fidelis  
—Dave Cannon*

# Acknowledgments

We would like to thank our Acquisitions Editor Jeff Kellum and Development Editor Lisa Bishop for their vision and guidance. Our Technical Editor Brady Pamplin was very helpful in providing his expert assistance during the writing of this book. We wish to thank Production Editor Rachel McConlogue for keeping the book on track, and for her tireless effort in ensuring that we put out the best book possible. We would also like to thank Copy Editor Sharon Wilkey, Compositor Craig Woods, Illustrators Mike Park and Jeffrey Wilson, Proofreader Jen Larsen, and Indexer Ted Laux for their polished efforts to make certain this second edition became a reality.



# Contents at a Glance

<i>Introduction</i>		<i>xix</i>
<i>Assessment Test</i>		<i>xxxii</i>
<b>Chapter 1</b>	Secrets of a Successful IS Auditor	1
<b>Chapter 2</b>	Audit Process	59
<b>Chapter 3</b>	IT Governance	117
<b>Chapter 4</b>	Networking Technology	183
<b>Chapter 5</b>	Life Cycle Management	253
<b>Chapter 6</b>	IT Service Delivery	323
<b>Chapter 7</b>	Information Asset Protection	369
<b>Chapter 8</b>	Disaster Recovery and Business Continuity	451
<b>Appendix A</b>	About the Companion CD	501
<b>Glossary</b>		505
<i>Index</i>		<i>547</i>





# Contents

*Introduction* *xix*

*Assessment Test* *xxxii*

<b>Chapter 1</b>	<b>Secrets of a Successful IS Auditor</b>	<b>1</b>
	Understanding the Demand for IS Audits	2
	Understanding Policies, Standards, Guidelines, and Procedures	6
	Understanding the ISACA Code of Professional Ethics	6
	Preventing Ethical Conflicts	8
	Understanding the Purpose of an Audit	9
	Classifying Basic Types of Audits	9
	Understanding the Auditor's Responsibility	10
	Comparing Audits to Assessments	10
	Auditor Role versus Auditee Role	11
	Applying an Independence Test	11
	Understanding the Various Auditing Standards	13
	Specific Regulations Defining Best Practices	16
	Identifying Specific Types of Audits	18
	Auditor Is an Executive Position	19
	Understanding the Importance of Auditor Confidentiality	19
	Working with Lawyers	20
	Retaining Audit Documentation	21
	Providing Good Communication and Integration	21
	Understanding Leadership Duties	22
	Planning and Setting Priorities	22
	Providing Standard Terms of Reference	23
	Dealing with Conflicts and Failures	24
	Identifying the Value of Internal and External Auditors	24
	Understanding the Evidence Rule	25
	Identifying Who You Need to Interview	26
	Understanding the Corporate Organizational Structure	27
	Identifying Roles in a Corporate Organizational Structure	27
	Identifying Roles in a Consulting Firm	
	Organizational Structure	29
	Managing Projects	31
	What Is a Project?	32
	What Is Project Management?	34
	Identifying the Requirements of a Project Manager	35
	Identifying a Project Manager's Authority	36
	Understanding the Project Management	
	Process Framework	36

	Applied Project Management Quick Reference	38
	Using Project Management Diagramming Techniques	45
	Summary	48
	Exam Essentials	48
	Review Questions	50
	Answers to Review Questions	56
<b>Chapter 2</b>	<b>Audit Process</b>	<b>59</b>
	Establishing and Approving an Audit Charter	60
	Role of the Audit Committee	62
	Engagement Letter	63
	Preplanning the Audit	63
	Identifying Restrictions on Scope	65
	Understanding the Variety of Audits	66
	Gathering Detailed Audit Requirements	66
	Using a Systematic Approach to Planning	68
	Comparing Traditional Audits to Assessments and Self-Assessments	69
	Choosing a Risk Management Strategy	70
	Performing an Audit Risk Assessment	73
	Determining Whether an Audit Is Possible	74
	Performing the Audit	74
	Allocating Staffing	75
	Ensuring Audit Quality Control	77
	Defining Auditee Communications	77
	Using Data Collection Techniques	78
	The Hierarchy of Internal Controls	80
	Reviewing Existing Controls	82
	Gathering Audit Evidence	85
	Using Evidence to Prove a Point	85
	Types of Evidence	86
	Typical Evidence for IS Audits	86
	Using Computer Assisted Audit Tools	87
	Electronic Discovery	89
	Grading of Evidence	90
	Timing of Evidence	92
	Evidence Life Cycle	93
	Preparing Audit Documentation	96
	Selecting Audit Samples	96
	Conducting Audit Testing	98
	Compliance Testing	98
	Substantive Testing	99
	Tolerable Error Rate	99
	Record Your Test Results	100

	Analyzing the Results	100
	Detecting Irregularities and Illegal Acts	101
	Reporting Your Audit Findings	103
	Identifying Omitted Procedures	104
	Conducting an Exit Interview	104
	Conducting Follow-Up Activities	105
	Summary	105
	Exam Essentials	105
	Review Questions	108
	Answers to Review Questions	114
<b>Chapter 3</b>	<b>IT Governance</b>	<b>117</b>
	Strategy Planning for Organizational Control	118
	Overview of the IT Steering Committee	120
	Using the Balanced Scorecard	125
	IT Subset of the BSC	128
	Selecting an IT Strategy	129
	Specifying a Policy	130
	Implementation Planning of the IT Strategy	131
	Using COBIT	134
	Identifying Sourcing Locations	134
	Conducting an Executive Performance Review	139
	Understanding the Auditor's Interest in the Strategy	139
	Overview of Tactical Management	139
	Planning and Performance	140
	Management Control Methods	140
	Project Management	143
	Risk Management	144
	Implementing Standards	146
	Human Resources	147
	System Life-Cycle Management	148
	Continuity Planning	149
	Insurance	149
	Performance Management	149
	Overview of Business Process Reengineering	150
	Why Use Business Process Reengineering	151
	BPR Methodology	152
	Genius or Insanity?	152
	Goal of BPR	153
	Guiding Principles for BPR	153
	Knowledge Requirements for BPR	154
	BPR Techniques	154
	BPR Application Steps	155
	Role of IS in BPR	158