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

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

Library of Congress Control Number: 2015960605

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

Contents