

Covers All Exam Objectives



Includes Real-World Scenarios, Hands-On Exercises,  
and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

# CISSP

## Certified Information Systems Security Professional STUDY GUIDE

Fifth Edition

James M. Stewart  
Ed Tittel  
Mike Chapple



SERIOUS SKILLS.



# **CISSP<sup>®</sup>**

# **Certified Information Systems Security Professional**

## **Study Guide**

## **Fifth Edition**





**CISSP®**  
**Certified Information Systems  
Security Professional**  
**Study Guide**  
**Fifth Edition**



James Michael Stewart  
Ed Tittel  
Mike Chapple



WILEY

Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum  
Development Editor: Rob Truhn  
Technical Editor: Darril Gibson  
Production Editor: Eric Charbonneau  
Copy Editor: Judy Flynn  
Editorial Manager: Pete Gaughan  
Production Manager: Tim Tate  
Vice President and Executive Group Publisher: Richard Swadley  
Vice President and Publisher: Neil Edde  
Media Project Manager 1: Laura Moss-Hollister  
Media Associate Producer: Shawn Patrick  
Media Quality Assurance: Marilyn Hummel  
Book Designer: Judy Fung  
Proofreader: Nancy Bell  
Indexer: Nancy Guenther  
Project Coordinator, Cover: Katie Crocker  
Cover Designer: Ryan Sneed

Copyright © 2011 by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-94498-1

ISBN: 978-1-118-02825-4 (ebk)

ISBN: 978-1-118-02827-8 (ebk)

ISBN: 978-1-118-02826-1 (ebk)

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 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. CISSP is a registered trademark of International Information Systems Security Certification Consortium, Inc. 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 *CISSP: Certified Information Systems Security Professional Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 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). 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,

A handwritten signature in black ink, appearing to read 'Neil Edde', with a stylized, flowing script.

Neil Edde  
Vice President and Publisher  
Sybex, an Imprint of Wiley





*To Cathy, whenever there is trouble, just remember “Some beach,  
somewhere . . .”*

*—James Michael Stewart*

*To my Mom, Cecilia Katherine: the world is not as bright without you in it  
anymore, and we all still miss you every day.*

*—Ed Tittel*

*To my family: Renee, Richard, Matthew, and Christopher, who lovingly put  
up with me during the hours I spent buried in my laptop writing this book.*

*—Mike Chapple*

# Acknowledgments

I hope our efforts to improve this study guide will lend themselves handily to your understanding and comprehension of the wide berth of CISSP concepts. I'd like to express my thanks to Sybex for continuing to support this project. Thanks to Ed Tittel and Mike Chapple for continuing to contribute to this project. Also thanks to all my CISSP course students who have provided their insight and input to improve my training courseware and ultimately this tome. Extra thanks to the 5th Edition Technical Editor, Darril Gibson, who performed amazing feats in guiding us to improve this book.

To my wonderful wife, Cathy, our life together is just getting started. To my son, Xzavier Slayde, and daughter, Remington Annaliese, may you grow to be more than we could imagine. To my parents, Dave and Sue, thanks for your love and consistent support. To Mark, as best friends go, it could've been worse. And finally, as always, to Elvis—all hail the King!

—*James Michael Stewart*

Thanks to both Michael Stewart and Mike Chapple for continuing to keep me involved in this project. Michael continues to teach CISSP courses with amazing frequency, which provides us with a lifeline to the hard-working professionals in the trenches for whom this credential means so much. Congrats again to Michael on another addition to his family; my son, Gregory, is now in first grade and the time just keeps flying by. May the months and years slip by as pleasantly and painlessly for you as they have for us. Next, thanks to the folks at Sybex, especially Jeff Kellum for rounding us all up and keeping us headed in the same direction and for his excellent view of where we need to take this book. Finally, I'd like to thank my loving and lovely wife, Dina, for all the great things she does to make family life so comfortable, clean, interesting and fun.

—*Ed Tittel*

Special thanks go to the information security team at the University of Notre Dame. Gary Dobbins, Bob Winding, David Seidl, and Robert Riley provided hours of interesting conversation and debate on security issues that inspired and informed much of the material in this book.

I would like to thank the team at Wiley who provided invaluable assistance throughout the book development process. I also owe a debt of gratitude to my literary agent, Carole Jelen of Waterside Productions. My coauthors, Ed Tittel and James Michael Stewart, have worked with me ever since we published the first edition of this book together eight years ago. I'd also like to thank the many people who participated in the production of this book but whom I never had the chance to meet: the graphics team, the production staff, and all of those involved in bringing this book to press.

—*Mike Chapple*

# About the Authors

**James Michael Stewart, CISSP**, has been writing and training for more than 16 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on Windows security and ethical hacking/penetration testing. He is the author of several books and courseware sets on security certification, Microsoft topics, and network administration. More information about Michael can be found at his website: [www.impactonline.com](http://www.impactonline.com).

**Ed Tittel** is a full-time freelance writer, trainer, and consultant specializing in matters related to information security, markup languages, and networking technologies. He is a regular contributor to numerous TechTarget websites (and keeps updating his security certification survey for SearchSecurity.com), teaches online security and technology courses for HP, and enjoys his occasional gigs as an expert witness on Web technologies from the mid-1990s when he was lucky enough to write a raft of books in that arena. Ed's professional bio and other information are available at [www.edtittel.com](http://www.edtittel.com).

**Mike Chapple, CISSP, PhD**, is an IT professional with the University of Notre Dame. In the past, he was chief information officer of Brand Institute and an information security researcher with the National Security Agency and the U.S. Air Force. His primary areas of expertise include network intrusion detection and access controls. Mike is a frequent contributor to TechTarget's SearchSecurity site and the author of several information security titles including *The GSEC Prep Guide* from Wiley and *Information Security Illuminated* from Jones and Bartlett Publishers.



# Contents at a Glance

<i>Introduction</i>	<i>xxix</i>
<b>Chapter 1</b>	Accountability and Access Control 1
<b>Chapter 2</b>	Attacks and Monitoring 49
<b>Chapter 3</b>	ISO Model, Protocols, Network Security, and Network Infrastructure 83
<b>Chapter 4</b>	Communications Security and Countermeasures 153
<b>Chapter 5</b>	Security Management Concepts and Principles 197
<b>Chapter 6</b>	Asset Value, Policies, and Roles 223
<b>Chapter 7</b>	Data and Application Security Issues 265
<b>Chapter 8</b>	Malicious Code and Application Attacks 321
<b>Chapter 9</b>	Cryptography and Symmetric Key Algorithms 365
<b>Chapter 10</b>	PKI and Cryptographic Applications 409
<b>Chapter 11</b>	Principles of Computer Design 447
<b>Chapter 12</b>	Principles of Security Models 489
<b>Chapter 13</b>	Administrative Management 537
<b>Chapter 14</b>	Auditing and Monitoring 571
<b>Chapter 15</b>	Business Continuity Planning 611
<b>Chapter 16</b>	Disaster Recovery Planning 641
<b>Chapter 17</b>	Law and Investigations 681
<b>Chapter 18</b>	Incidents and Ethics 717
<b>Chapter 19</b>	Physical Security Requirements 747
<b>Appendix</b>	About the Companion CD 785
<i>Index</i>	<i>789</i>



# Contents

*Introduction*

*xxix*

<b>Chapter 1</b>	<b>Accountability and Access Control</b>	<b>1</b>
	Access Control Overview	2
	Types of Access Control	3
	Access Control in a Layered Environment	5
	The Process of Accountability	6
	Identification and Authentication Techniques	10
	Passwords	11
	Biometrics	14
	Tokens	19
	Tickets	21
	Single Sign-On	21
	Access Control Techniques	24
	Discretionary Access Controls	25
	Nondiscretionary Access Controls	25
	Mandatory Access Controls	26
	Role-Based Access Control	27
	Lattice-Based Access Controls	28
	Access Control Methodologies and Implementation	29
	Centralized and Decentralized Access Control	29
	RADIUS and TACACS	30
	Access Control Administration	31
	Account Administration	31
	Account, Log, and Journal Monitoring	32
	Access Rights and Permissions	33
	Summary	37
	Exam Essentials	38
	Written Lab	40
	Answers to Written Lab	41
	Review Questions	42
	Answers to Review Questions	46
<b>Chapter 2</b>	<b>Attacks and Monitoring</b>	<b>49</b>
	Monitoring	50
	Intrusion Detection	52
	Host- and Network-Based IDSs	54
	Knowledge- and Behavior-Based Detection	56
	IDS-Related Tools	57
	Understanding Honeypots	58