Information Technology Control and Audit

Third Edition

Sandra Senft ◆ Frederick Gallegos

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Information Technology Control and Audit

Third Edition

Sandra Senft ◆ Frederick Gallegos

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2009 by Taylor & Francis Group, LLC
Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-6550-3 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

Information Technology Control and Audit

Third Edition

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Architecting Secure Software Systems
Asoke K. Talukder and Manish Chaitanya
ISBN: 978-1-4200-8784-0

Building an Effective Information Security Policy Architecture
Sandy Bacik
ISBN: 978-1-4200-5905-2

CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives
Ron Collette, Michael Gentile and Skye Gentile
ISBN: 978-1-4200-8910-3

Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies
Tyson Macaulay
ISBN: 978-1-4200-6835-1

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition
Albert Marcella, Jr. and Doug Menendez
ISBN: 978-0-8493-8328-1

Digital Privacy: Theory, Technologies, and Practices
Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis and Sabrina di Vimercati
ISBN: 978-1-4200-5217-6

How to Achieve 27001 Certification: An Example of Applied Compliance Management
Sigurjon Thor Arnason and Keith D. Willett
ISBN: 978-0-8493-3648-5

How to Complete a Risk Assessment in 5 Days or Less
Thomas R. Peltier
ISBN: 978-1-4200-6275-5

Information Assurance Architecture
Keith D. Willett
ISBN: 978-0-8493-8067-9

Information Security Management Handbook, Sixth Edition
Harold F. Tipton and Micki Krause, Editors
ISBN: 978-0-8493-7495-1

Information Technology Control and Audit, Third Edition
Sandra Senft and Frederick Gallegos
ISBN: 978-1-4200-6550-3

Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks
Kenneth Brancik
ISBN: 978-1-4200-4659-5

IT Auditing and Sarbanes-Oxley Compliance: Key Strategies for Business Improvement
Dimitris N. Chorafas
ISBN: 978-1-4200-8617-1

Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet
Ken Dunham and Jim Melnick
ISBN: 978-1-4200-6903-7

Mechanics of User Identification and Authentication: Fundamentals of Identity Management
Dobromir Todorov
ISBN: 978-1-4200-5219-0

Oracle Identity Management: Governance, Risk, and Compliance Architecture, Third Edition
Marlin B. Pohlman
ISBN: 978-1-4200-7247-1

Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking
Silvio Ciappi and Stefania Ducci
ISBN: 978-1-4200-8693-5

Security in an IPv6 Environment
Daniel Minoli and Jake Kouns
ISBN: 978-1-4200-9229-5

Security Software Development: Assessing and Managing Security Risks
Douglas A. Ashbaugh
ISBN: 978-1-4200-6380-6

Software Deployment, Updating, and Patching
Bill Stackpole and Patrick Hanrion
ISBN: 978-0-8493-5800-5

Understanding and Applying Cryptography and Data Security
Adam J. Elbirt
ISBN: 978-1-4200-6160-4

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

此为试读,需要完整PDF请访问: www.ertongbook.com

Preface

This book is designed to meet the increasing need of audit and control professionals to understand information technology (IT) and the controls required to manage this key resource. This book can be used by control and audit professionals and for both introductory and advanced courses in IT audit. This book supports the Control Objectives for Information and Related Technology (CobiT) model and assists in preparation for the Certified Information Systems Auditor (CISA) exam. Exhibit 1 provides a map of this text to the CISA exam.

Exhibit 1 Mapping Text to CISA Exam

Exam (%)	*CISA Examination Content Areas to Model Curriculum (Undergraduate)* — *Title and Description*	*IT Audit and Control*	*IT Planning and Organization*	*IT Acquisition and Implementation*	*IT Delivery and Support*	*Advanced Topics*
10	*The IS audit process* Provides IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its IT and business systems are protected and controlled	X				
15	*IT governance* Provides assurance that the organization has the structure, policies, accountability, mechanisms, and monitoring practices in place to achieve the requirements of corporate governance of IT	X	X			

(*continued*)

Exhibit 1 Continued

Exam (%)	*CISA Examination Content Areas to Model Curriculum (Undergraduate)* — *Title and Description*	*IT Audit and Control*	*IT Planning and Organization*	*IT Acquisition and Implementation*	*IT Delivery and Support*	*Advanced Topics*
16	*Systems and infrastructure life-cycle management* Provides assurance that the management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the organization's objectives		X	X		
14	*IT service delivery and support* Provides assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives		X	X	X	
31	*Protection of information assets* Provides assurance that the security architecture (policies, standards, procedures, and controls) ensures the confidentiality, integrity, and availability of information assets		X	X	X	X
14	*Business continuity and disaster recovery* Provides assurance that in the event of a disruption the business continuity and disaster recovery processes will ensure the timely resumption of IT services while minimizing the business impact			X	X	

Acknowledgments

The authors of this book have many to thank for the support they received in preparation of this book. Our combined 50 years of information systems (IS) audit, control, and security experience includes four books, over 200 professional articles, and 200 presentations in this field. This book is designed for those who wish to learn and possibly select this field as their profession and those who wish to retool and enhance their audit tool kit with new experiences and techniques. In essence, we have collected our past experiences, successes, and lessons learned. We hope you will profit from this book and share it with your colleagues.

We thank our editor, Ray O'Connell, for having supported this effort. We wish to thank the IS Audit and Information Assurance Faculty worldwide who have been in the trenches to teach this profession to the many who want to learn what it is all about. The research and writings of Professors A. Faye Borthick, Ron Weber, Roger Jamieson, John Wyber, Alan Friedberg, Dan Kneer, Nils Kandelin, Tommie Singleton, Sokratis Katsikas, Gary McCombs, Damaso Lopez, Howard Kanter, Karen Forcht, Alan T. Lord, Joe Gelinas, Kil C. Kim, Hiroshi Yoshida, Jae Up Kim, Josef Vyskoc, Gordon B. Davis, Elsie Jancura, Corey Schou, Carol Sledge, Peter Best, and many more have been helpful to the field of Information Technology Audit, Control and Security. This book is in memorandum to the professionals in the past who paved the way: Joseph Wasserman, Harold J. Highland, Wayne Snipes, Keagle Davis, Stan Halper, Francis Langlinais, and Donald C. Scantlebury; and in honor of those professionals who continue the search for excellence in this field: John Lainhart IV, Robert B. Parker, Michael Cangemi, Steven Ross, Steven Jue, Art Foreman, David Irvin, Nick Horsky, William Perry, Bill Mair, Donald Wood, Carl Pabst, John Kuyers, Dana "Rick" Richardson, Belden Menkus, Robert Roussey, Akira Matsuo, Paul Williams, Fred Lilly, Michael Parkinson, John Beveridge, Michael Villegas, Hugh H. Peri-Williams, Hugh Parkes, John Tongren, and many, many more.

We also thank our past and current employers for giving us the opportunity to experience this challenging environment and excel in our IS audit careers; the U.S. General Accounting Office, now the Government Accountability Office (GAO), Coldwell Banker, Avery International, Mc Donnell Douglas, Farmers Insurance, and Zurich Financial Services. Finally, the involvement and experience with the professional associations worldwide that support this field, which is mentioned in this book for their many contributions, especially those members of the Information Systems Audit and Control Association (ISACA) Model Curriculum Task Force and Academic Relations Committee and their initial product, which was issued in March 1998, and the Follow-on Model Revision Task Force effort led by Dr. Alan Lord issued in 2005.

We also thank our colleagues, alumni, and students for their participation and contributions to the writings and editing of this work. We thank Professors Steven Powell, Louise Soe, Koichiro Isshiki, Larisa Preiser-Houy, Steven Curl, Ida Masouris, Ruth Guthrie, Ward Testerman, Dan Manson, Carol Heins-Gonzales, Anna Carlin for their written contributions; and technical review by IT Professionals Roger Lux, Paul Senft, Juan Ossa, and Robert Carter. We thank alumnis Mattie Woods, Scott Kandel, Roin Nance, Matt Touquet, Karen Seketa, Kevin Powell, Dan Dow, Amin Leiman, Larry Lam, Richard Leonard, Ron Proulx, Harry Soo, Charles Bent, Tessa Rogge,

David Wright, Lana Nino, Karen Nelson, Gerald Morris, Henry Townsend, John Carvala, Steven Barnes, Debbie Newman, Isabelle Prieve-Theisen, Christine Kartawidjaja, Lidya Kartawidjaja, Heru Subroto, —Nurullah Askan, Gatu Prihartoyo, Kim Phelps-Kneough, Paul Wan, Boulton Fernando, Waberyn Wambugi, Rosina Liu, Loida Tison-Dualan, Seth Cox, Randy Coneby, Lorne Dear, Phoung Quach, Benny Hsu, Amanda Xu, Edson Gin, Matt Smith, Kevin Butscher, Rodney Kocot, Alex Li, Genemar Lazo, Stephen Sun, Sean Liu, Arthur Estillore, Martin Rojas, Matt Meyers, Allison Delpit, Bill Liao, Adi Dzaferovich, Brandon Brown, Sheryl Benedict, Charles Chantakrivat, and over 300 others whom we have placed into the IS audit profession.

We thank our current students at the undergraduate and graduate level, and special thanks to Mohammad Al-Abdullah, Stephanie Doda, Edson Gin, and Steven Tanner for their assistance and support. We also wish to thank our faculty Kathleen Von Velasco, Martha Guarnett, Fritzi Taylor, and Victoria Galvez for their support.

This work is a combined effort of the many we have worked with, the many we have shared with, and the many we have taught to go on into this profession worldwide. We hope you will use it and add to it in your professional development in this exciting field.

Authors

Frederick Gallegos, MBA, CGFM, has expertise in IT Audit Education, IS Auditing, Security, and Control of Information Systems; Legal Environment of Information Systems; Local Area and Wide Area Network Security and Controls; Computer Ethics, Management Information Systems, Executive Support Systems, Internet as an Audit Resource. He has more than 35 years of teaching and practical experience in the field, published four books, and authored and coauthored more than 200 articles in the aforementioned subjects. He received his BS and MS from the California State Polytechnic University, Pomona, California. He is a Certified Government Financial Manager (CGFM) and has a California Community College Instructor Credential. He taught for the Computer Information Systems Department, College of Business at California State Polytechnic University, Pomona, California, from 1976 to 1996 (part-time) and full-time from 1996 to 2006. After 30 years of teaching, he retired in September 2006 and received the lecturer emeritus status from the university in May 2007. In February 2008, he received the Computer Information Systems (CIS) Lifetime Achievement Award from the CIS Department at Cal Poly, Pomona, California. He continues to maintain contact with his past undergraduate and graduate students and alumni of the CIS Department's Information Assurance programs from the California State Polytechnic University, Pomona, California.

Before teaching full-time at Cal Poly (1996–2006), Gallegos worked for GAO—Los Angeles Regional Office (1972–1996) and advanced within GAO to serve as manager, Management and Evaluator Support Group. He managed staff involved in Office Automation, Computer Audit Support, Computer Audit, Training, Human Resource Planning and Staffing, Technical Information Retrieval and Security/Facilities Management. He retired from GAO in 1996 with 26 years of federal and military service. He is a recipient of several service awards from GAO, EDP Audit, Control, and Security Newsletter (EDPACS), and ISACA that recognized his past contributions to the field and his efforts in the establishment of formal universities courses at his *alma mater* in IS Auditing, Control and Security at the undergraduate level in 1979 with the implementation of Association to Advance Collegiate Schools of Business (AACSB) accredited graduate-level Master of Science in Business Administration Degree program in IS Auditing since 1980. (The AACSB was founded in 1916 to accredit schools of business worldwide.) Gallegos has spoken widely on topics related to the IS Audit, Control, and Security field. He served in a number of assignments and positions with the ISACA in the past. They are as follows:

- *ISACA Foundation*. Member of the Standards Board and Committee (1984–1996), involved in the issuance of general standards for the EDP audit profession and named as contributor for the general standards and nine IS audit standards
- *ISACA*. Member of the History Committee (1986–2006)
- Involved in writing the history of EDP Auditors Association for the 25th anniversary
- Editorial Board Member for *ISACA Journal* (1995–2006)
- Member of the Academic Liaison Committee (1984–1990, 1995–1997)

- *Chair, President's Task Force.* ISACA for the development of curricula for undergraduate and graduate education in IS auditing (May 1995—issued March 1998) and member of the second task force for the revision of the ISACA Model, issued 2004

Gallegos is also a member of the Association of Government Accountants.

Sandra Senft, MSBA-IS Audit, CISA, CIA, is an executive with more than 25 years of combined experience in auditing, financial management, insurance, and IS. Recently, she held the global role of chief financial officer for Group IT within Zurich Financial Services in Zurich, Switzerland. During her career in IT, her responsibilities included controlling, process improvement, project management, quality management, service management, sourcing, and vendor management.

Senft's extensive understanding of the IT and financial disciplines was further developed as an IS auditor from 1993 to 1999, specializing in auditing systems development projects as well as general control audits of mainframe and distributed systems, information security, disaster recovery, and quality assurance. She was also responsible for defining and developing the audit risk methodology, audit methodology, documenting processes, and training audit staff. She was the lead in defining requirements and selecting the technology to automate the audit workflow.

A faculty member of California State Polytechnic University, Pomona, California, from 1997 to 2000, she taught undergraduate and graduate courses in IT and IS auditing. She has also presented IS auditing topics at seminars, conferences, and CISA review courses specializing in systems development auditing. She has authored and coauthored several articles on IT controls and audit for Auerbach Publications.

Senft graduated from California State Polytechnic University, Pomona, California, with a Master of Science in business administration option in IS auditing and a Bachelor of Science in accounting. She is a Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), and Competent Toastmaster (CTM). She served as president, treasurer, director of research and academic relations, and spring conference chair for the Los Angeles Chapter of ISACA.

此为试读,需要完整PDF请访问: www.ertongbook.com

Contents

此为试读,需要完整PDF请访问: www.ertongbook.com