

WILEY CORPORATE F&A

AUDITOR'S GUIDE TO IT AUDITING

Second Edition

RICHARD CASCARINO

Auditor's Guide to IT Auditing

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Corporate F&A series provides information, tools, and insights to corporate professionals responsible for issues affecting the profitability of their company, from accounting and finance to internal controls and performance management.

Auditor's Guide to IT Auditing

Second Edition

RICHARD E. CASCARINO



WILEY

John Wiley & Sons, Inc.

Copyright © 2012 by Richard E. Cascarino. All rights reserved.
Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

First Edition: Auditor's Guide to Information Systems Auditing (978-0-470-00989-5). Copyright © 2007
John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. 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: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States 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. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Cascarino, Richard.

Auditor's guide to IT auditing / Richard E. Cascarino. — 2nd ed.

p. cm. — (Wiley corporate F&A series)

Rev. ed. of: Auditor's guide to information systems auditing.

Includes index.

ISBN 978-1-118-14761-0 (hardback); ISBN 978-1-118-22584-4 (ebk);

ISBN 978-1-118-23907-0 (ebk); ISBN 978-1-118-24425-8 (ebk)

1. Electronic data processing—Auditing. I. Cascarino, Richard. Auditor's guide to information systems auditing. II. Title.

QA76.9.A93C37 2012

658'.0558—dc23

2011042683

ISBN 978-1118-14761-0

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1


I wish to take this opportunity to dedicate this book to my wife, Max, who has, over the last 33 years, put up with my bad temper when the computer would not do what I programmed it to do, my ego when it did eventually work, my despair when the system crashed again and again, and my complacency when the problems were solved.

I would also like to thank those who molded my career over the years, particularly Jim Leary for showing me what an IS manager could be and Scotch Duncan Anderson for showing me what an internal auditor should be.

And in grateful thanks to my friend, the late Gene Schultz, who died before being able to review the second edition of this book having given such a sterling review to the first edition. He was an inspiration and will be sadly missed.


Contents


Preface xvii

	PART I: IT AUDIT PROCESS	1
	Chapter 1: Technology and Audit	3
	Technology and Audit	4
	Batch and Online Systems	8
	Electronic Data Interchange	20
	Electronic Business	21
	Cloud Computing	22
	Chapter 2: IT Audit Function Knowledge	25
	Information Technology Auditing	25
	What Is Management?	26
	Management Process	26
	Understanding the Organization's Business	27
	Establishing the Needs	27
	Identifying Key Activities	27
	Establish Performance Objectives	27
	Decide the Control Strategies	27
	Implement and Monitor the Controls	28
	Executive Management's Responsibility and Corporate Governance	28
	Audit Role	28
	Conceptual Foundation	29
	Professionalism within the IT Auditing Function	29
	Relationship of Internal IT Audit to the External Auditor	30
	Relationship of IT Audit to Other Company Audit Activities	30
	Audit Charter	30
	Charter Content	30
	Outsourcing the IT Audit Activity	31
	Regulation, Control, and Standards	31

Chapter 3: IT Risk and Fundamental Auditing Concepts	33
Computer Risks and Exposures	33
Effect of Risk	35
Audit and Risk	36
Audit Evidence	37
Conducting an IT Risk-Assessment Process	38
NIST SP 800 30 Framework	38
ISO 27005	39
The “Cascarino Cube”	39
Reliability of Audit Evidence	44
Audit Evidence Procedures	45
Responsibilities for Fraud Detection and Prevention	46
Notes	46
Chapter 4: Standards and Guidelines for IT Auditing	47
IIA Standards	47
Code of Ethics	48
Advisory	48
Aids	48
Standards for the Professional Performance of Internal Auditing	48
ISACA Standards	49
ISACA Code of Ethics	50
COSO: Internal Control Standards	50
BS 7799 and ISO 17799: IT Security	52
NIST	53
BSI Baselines	54
Note	55
Chapter 5: Internal Controls Concepts Knowledge	57
Internal Controls	57
Cost/Benefit Considerations	59
Internal Control Objectives	59
Types of Internal Controls	60
Systems of Internal Control	61
Elements of Internal Control	61
Manual and Automated Systems	62
Control Procedures	63
Application Controls	63
Control Objectives and Risks	64
General Control Objectives	64
Data and Transactions Objectives	64
Program Control Objectives	66
Corporate IT Governance	66
COSO and Information Technology	68
Governance Frameworks	70
Notes	71

Chapter 6: Risk Management of the IT Function	73
Nature of Risk	73
Risk-Analysis Software	74
Auditing in General	75
Elements of Risk Analysis	77
Defining the Audit Universe	77
Computer System Threats	79
Risk Management	80
Notes	83
Chapter 7: Audit Planning Process	85
Benefits of an Audit Plan	85
Structure of the Plan	89
Types of Audit	91
Chapter 8: Audit Management	93
Planning	93
Audit Mission	94
IT Audit Mission	94
Organization of the Function	95
Staffing	95
IT Audit as a Support Function	97
Planning	97
Business Information Systems	98
Integrated IT Auditor versus Integrated IT Audit	98
Auditees as Part of the Audit Team	100
Application Audit Tools	100
Advanced Systems	100
Specialist Auditor	101
IT Audit Quality Assurance	101
Chapter 9: Audit Evidence Process	103
Audit Evidence	103
Audit Evidence Procedures	103
Criteria for Success	104
Statistical Sampling	105
Why Sample?	106
Judgmental (or Non-Statistical) Sampling	106
Statistical Approach	107
Sampling Risk	107
Assessing Sampling Risk	108
Planning a Sampling Application	109
Calculating Sample Size	111
Quantitative Methods	111
Project-Scheduling Techniques	116
Simulations	117



Computer-Assisted Audit Solutions	118
Generalized Audit Software	118
Application and Industry-Related Audit Software	119
Customized Audit Software	120
Information-Retrieval Software	120
Utilities	120
On-Line Inquiry	120
Conventional Programming Languages	120
Microcomputer-Based Software	121
Test Transaction Techniques	121
Chapter 10: Audit Reporting Follow-up	123
Audit Reporting	123
Interim Reporting	124
Closing Conferences	124
Written Reports	124
Clear Writing Techniques	125
Preparing to Write	126
Basic Audit Report	127
Executive Summary	127
Detailed Findings	128
Polishing the Report	129
Distributing the Report	129
Follow-up Reporting	129
Types of Follow-up Action	130
 PART II: INFORMATION TECHNOLOGY GOVERNANCE	131
Chapter 11: Management	133
IT Infrastructures	133
Project-Based Functions	134
Quality Control	138
Operations and Production	139
Technical Services	140
Performance Measurement and Reporting	140
Measurement Implementation	141
Notes	145
Chapter 12: Strategic Planning	147
Strategic Management Process	147
Strategic Drivers	148
New Audit Revolution	149
Leveraging IT	149
Business Process Re-Engineering Motivation	150
IT as an Enabler of Re-Engineering	151
Dangers of Change	152
System Models	152

Information Resource Management	153
Strategic Planning for IT	153
Decision Support Systems	155
Steering Committees	156
Strategic Focus	156
Auditing Strategic Planning	156
Design the Audit Procedures	158
Note	158
Chapter 13: Management Issues	159
Privacy	161
Copyrights, Trademarks, and Patents	162
Ethical Issues	162
Corporate Codes of Conduct	163
IT Governance	164
Sarbanes-Oxley Act	166
Payment Card Industry Data Security Standards	166
Housekeeping	167
Notes	167
Chapter 14: Support Tools and Frameworks	169
General Frameworks	169
COSO: Internal Control Standards	172
Other Standards	173
Governance Frameworks	176
Note	178
Chapter 15: Governance Techniques	179
Change Control	179
Problem Management	181
Auditing Change Control	181
Operational Reviews	182
Performance Measurement	182
ISO 9000 Reviews	184
 PART III: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT	185
Chapter 16: Information Systems Planning	187
Stakeholders	187
Operations	188
Systems Development	189
Technical Support	189
Other System Users	191
Segregation of Duties	191
Personnel Practices	192
Object-Oriented Systems Analysis	194

Enterprise Resource Planning	194
Cloud Computing	195
Notes	197
Chapter 17: Information Management and Usage	199
What Are Advanced Systems?	199
Service Delivery and Management	201
Computer-Assisted Audit Tools and Techniques	204
Notes	205
Chapter 18: Development, Acquisition, and Maintenance of Information Systems	207
Programming Computers	207
Program Conversions	209
No Thanks Systems Development Exposures	209
Systems Development Controls	210
Systems Development Life Cycle Control: Control Objectives	210
Micro-Based Systems	212
Cloud Computing Applications	212
Note	213
Chapter 19: Impact of Information Technology on the Business Processes and Solutions	215
Impact	215
Continuous Monitoring	216
Business Process Outsourcing	218
E-Business	219
Notes	220
Chapter 20: Software Development	221
Developing a System	221
Change Control	225
Why Do Systems Fail?	225
Auditor's Role in Software Development	227
Chapter 21: Audit and Control of Purchased Packages and Services	229
IT Vendors	230
Request For Information	231
Requirements Definition	231
Request for Proposal	232
Installation	233
Systems Maintenance	233
Systems Maintenance Review	234
Outsourcing	234
SAS 70 Reports	234

Chapter 22: Audit Role in Feasibility Studies and Conversions	237
Feasibility Success Factors	237
Conversion Success Factors	240
Chapter 23: Audit and Development of Application Controls	243
What Are Systems?	243
Classifying Systems	244
Controlling Systems	244
Control Stages	245
Control Objectives of Business Systems	245
General Control Objectives	246
CAATs and Their Role in Business Systems Auditing	247
Common Problems	249
Audit Procedures	250
CAAT Use in Non-Computerized Areas	250
Designing an Appropriate Audit Program	250
PART IV: INFORMATION TECHNOLOGY SERVICE DELIVERY AND SUPPORT	253
Chapter 24: Technical Infrastructure	255
Auditing the Technical Infrastructure	257
Infrastructure Changes	259
Computer Operations Controls	260
Operations Exposures	261
Operations Controls	261
Personnel Controls	261
Supervisory Controls	262
Information Security	262
Operations Audits	263
Notes	264
Chapter 25: Service-Center Management	265
Private Sector Preparedness (PS Prep)	266
Continuity Management and Disaster Recovery	266
Managing Service-Center Change	269
Notes	269
PART V: PROTECTION OF INFORMATION ASSETS	271
Chapter 26: Information Assets Security Management	273
What Is Information Systems Security?	273
Control Techniques	276
Workstation Security	276

Physical Security	276
Logical Security	277
User Authentication	277
Communications Security	277
Encryption	277
How Encryption Works	278
Encryption Weaknesses	279
Potential Encryption	280
Data Integrity	280
Double Public Key Encryption	281
Steganography	281
Information Security Policy	282
Notes	282
Chapter 27: Logical Information Technology Security	283
Computer Operating Systems	283
Tailoring the Operating System	284
Auditing the Operating System	285
Security	286
Criteria	286
Security Systems: Resource Access Control Facility	287
Auditing RACF	288
Access Control Facility 2	289
Top Secret	290
User Authentication	291
Bypass Mechanisms	293
Security Testing Methodologies	293
Notes	295
Chapter 28: Applied Information Technology Security	297
Communications and Network Security	297
Network Protection	298
Hardening the Operating Environment	300
Client Server and Other Environments	301
Firewalls and Other Protection Resources	301
Intrusion-Detection Systems	303
Note	304
Chapter 29: Physical and Environmental Security	305
Control Mechanisms	306
Implementing the Controls	310

 PART VI: BUSINESS CONTINUITY AND DISASTER RECOVERY	311
Chapter 30: Protection of the Information Technology Architecture and Assets: Disaster-Recovery Planning	313
Risk Reassessment	314
Disaster—Before and After	315
Consequences of Disruption	317
Where to Start	317
Testing the Plan	319
Auditing the Plan	320
Chapter 31: Displacement Control	323
Insurance	323
Self-Insurance	327
 PART VII: ADVANCED IT AUDITING	329
Chapter 32: Auditing E-commerce Systems	331
E-Commerce and Electronic Data Interchange: What Is It?	331
Opportunities and Threats	332
Risk Factors	335
Threat List	335
Security Technology	336
“Layer” Concept	336
Authentication	336
Encryption	337
Trading Partner Agreements	338
Risks and Controls within EDI and E-Commerce	338
E-Commerce and Auditability	340
Compliance Auditing	340
E-Commerce Audit Approach	341
Audit Tools and Techniques	341
Auditing Security Control Structures	342
Computer-Assisted Audit Techniques	343
Notes	343
Chapter 33: Auditing UNIX/Linux	345
History	345
Security and Control in a UNIX/Linux System	347
Architecture	348
UNIX Security	348
Services	349
Daemons	350
Auditing UNIX	350
Scrutiny of Logs	351
Audit Tools in the Public Domain	351

UNIX Password File	352
Auditing UNIX Passwords	353
Chapter 34: Auditing Windows VISTA and Windows 7	355
History	355
NT and Its Derivatives	356
Auditing Windows Vista/Windows 7	357
Password Protection	358
VISTA/Windows 7	359
Security Checklist	359
Chapter 35: Foiling the System Hackers	361
Chapter 36: Preventing and Investigating Information Technology Fraud	367
Preventing Fraud	367
Investigation	369
Identity Theft	376
Note	376
Appendix A Ethics and Standards for the IS Auditor	377
ISACA Code of Professional Ethics	377
Relationship of Standards to Guidelines and Procedures	378
Appendix B Audit Program for Application Systems Auditing	379
Appendix C Logical Access Control Audit Program	393
Appendix D Audit Program for Auditing UNIX/Linux Environments	401
Appendix E Audit Program for Auditing Windows VISTA and Windows 7 Environments	407
About the Author	415
About the Website	417
Index	419

Preface

IN TODAY'S BUSINESS ENVIRONMENT, computers are continuing the revolution started in the 1950s. Size and capacity of the equipment grows on an exponential curve, with the reduction in cost and size ensuring that organizations take advantage of this to develop more effective and responsive systems, which allow them to seek to gain competitive advantage by interfacing more closely with their customers. This second edition has been brought up to date with the latest in information technology (IT) approaches such as cloud computing as well as the latest in standards and regulations. The section on risk management has been expanded to include varying risk-analysis techniques available to the IT auditor.

Net technologies such as cloud computing, electronic data interchange (EDI), electronic funds transfers (EFTs), and e-commerce have fundamentally changed the nature of business itself and, as a result, organizations have become more computer dependent. The radical changes to business are matched only by their impact on society.

It has become impossible for today's enterprises of any size and in any market sector to exist without computers to assist with their fundamental business operations. Even the old adage that "we can always go back to manual operations" is today a fallacy. The nature of today's business environment obviates that option. Even the smallest businesses have found that the advent of personal computers (PCs) with increased capabilities and processing speed, while at the same time reduced pricing and sophisticated PC software, has revolutionized the concept of what a small business is.

In order for organizations to take full advantage of the new facilities that computers can offer, it is important that their systems can be controlled and are dependable. They require that their auditors confirm that this is the case. The modern auditor therefore requires significantly more knowledge of computers and computer auditing than did auditors of earlier years.

CONTROLS IN MODERN COMPUTER SYSTEMS

The introduction of the computer has brought fundamental changes to the ways organizations process data. Computer systems:

- Are frequently much more complex than manual systems, the larger systems at least requiring a number of highly skilled computer technicians to develop and maintain them.
- Process large volumes of data at high speed, and can transmit data effectively and instantaneously over extreme distances, commonly between continents.
- Hold data in electronic form, which, without the appropriate tools and techniques, is often more complex for the auditor to access than paper records. In addition, modern systems have reduced the volumes of printed outputs by the incorporation of online access and online inquiry facilities. Indeed, many modern EDI-type systems have no paper audit trail whatsoever.
- Process data with much less manual intervention than manual systems. In fact large parts of sophisticated systems now process data with no manual intervention at all. In the past, the main justification for computerization was frequently to reduce the number of staff required to operate the business. With modern decision support and integrated systems, this is becoming a reality not at the clerical level, but at the decision-making and control level. This can have the effect that the fundamental business controls previously relied upon by the auditor, such as segregation of duties or management authorization, may no longer be carried out as previously and must be audited in a different manner. In computer systems, the user profile of the member of staff as defined within the system's access rights will generally control the division of duties while managerial authorities are, in many cases, built into systems themselves.
- Process consistently in accordance with their programs providing the computer has been programmed correctly and change control is effective.
- In large minicomputer and mainframe systems, there is a significant concentration of risk in locating the organization's information resources in one format, although not necessarily in one place. Organizations then become totally reliant on their computer system and must be able to recover from failure or the destruction of their computer system swiftly and with minimal business disruption.
- Are often subject to different legal constraints and burdens of proof than manual systems.
- May operate within a cloud environment within which control over the availability, security, and confidentiality of systems and data may be handed over to a third party and may be subject to laws of a differing country.

These changes brought about by computerization can greatly increase the opportunity for auditors to deliver a quality service by concentrating the risk and allowing the auditors to correspondingly concentrate their efforts. For example, harnessing the power of the computer to analyze large volumes of data in the way the auditor requires is commonly now the only practical way of analyzing corporate data, and this was not only impractical but also impossible while data was spread around the organization in a myriad of forms.

In addition, the use of computer systems with built-in programmed procedures permit the auditor to adopt a systems approach to auditing in that the controls within

the computer system process in a more consistent manner than a manual system. In manual systems the quality of the control procedure can change on a day-by-day basis, depending on the quality of the staff and their consistency of working. This can result in the auditor having to undertake a substantial amount of checking of transactions, to confirm transactions have processed correctly.

Controls within computer systems are commonly classified in two main subdivisions:

1. **General controls.** The controls governing the environment in which the computer system is developed, maintained, and operated, and within which the application controls operate. These controls include the systems-development standards operated by the organization, the controls that apply to the operation of the computer installation, and those governing the functioning of systems software. They have a pervasive effect on all application systems.
2. **Application controls.** The controls, both manual and computerized, within the business application to ensure that data is processed completely, accurately, and in a timely manner. Application controls are typically specific to the business application and include:
 - Input controls such as data validation and batching
 - Run-to-run controls to check file totals at key stages in processing, and controls over output

Ultimately, the auditor's job is to determine if the application systems function as intended, the integrity, accuracy, and completeness of the data is well controlled, and report any significant discrepancies. The integrity of the data relies on the adequacy of the application controls. However, application controls are totally dependent on the integrity of the general controls over the environment within which the application is developed and run.

In the past, the auditor has often assumed a considerable degree of reliance on controls around the computer, that is, in the application controls. This is sometimes referred to as auditing "around" the computer because the auditor concentrates on the input and output from the computer, rather than what happens in the computer.

This has never been truly justified but has become, over recent years, a lethal assumption.

With the spread of online and real-time working, and of the increasing capacity of fixed disks, all of the organization's data is commonly permanently loaded on the computer system and accessible from a variety of places, with only systems software controls preventing access to the data. This system is increasing in technical complexity, and the ability to utilize any implemented weaknesses is also growing.

It is critical that the auditor is assured of the integrity of the computer operational environment within which the applications systems function. This means that the auditor must become knowledgeable of the facilities provided in key systems software in the organization being audited.

This book is designed for those who need to gain a practical working knowledge of the risks and control opportunities within an IT environment, and the auditing of that

environment. Readers who will find the text particularly useful include professionals and students within the fields of:

- IT security
- IT audit
- Internal audit
- External audit
- Management information systems
- General business management

Overall, this book contains the information required by anyone who is, or expects to be, accountable to management for the successful implementation and control of information systems.

It is intended that the text within this book forms the foundation for learning experience, as well as being your reference manual and student text. The emphasis is therefore on both the principles and techniques as well as the practical implementation through the use of realistic case studies.

OVERALL FRAMEWORK

Within the book the terms Information Technology (IT) and Information Systems (IS) are both used because both are in common use to mean virtually identical functions. The book is split into eight parts, namely:

Part I: IT Audit Process

This part covers the introduction to the technology and auditing involved with the modern computer systems. It seeks to establish common frames of reference for all IT students by establishing a baseline of technological understanding as well as an understanding of risks, control objectives, and standards, all concepts essential to the audit function. Internal control concepts and the planning and management of the audit process in order to obtain the appropriate evidence of the achievement of the control objectives is explained as is the audit reporting process.

Chapter 1 covers the basics of technology and audit. The chapter is intended to give readers an understanding of the technology in use in business as well as knowledge of the jargon and its meaning. It covers the components of control within an IT environment and explains who the main players are and what their role is within this environment.

Chapter 2 looks at the laws and regulations governing IT audit and the nature and role of the audit charter. It reviews the varying nature of audit and the demand for audits as well as the need for control and audit of computer-based IS. The types of audit and auditor and range of services to be provided are reviewed together with the standards and codes of ethics of both the Institute of Internal Auditors (IIA) and the standards specified by the Information Systems Audit and Control Association (ISACA).

Chapter 3 explores the concepts of materiality and risk within the IT audit function and contrasts materiality as it is commonly applied to financial statement audit such as those performed by independent external auditors. In this context, the quality and types of evidence required to meet the definitions of sufficiency, reliability, and relevancy are examined. The risks involved in examining evidence to arrive at an audit conclusion are reviewed as are the need to maintain the independence and objectivity of the auditor and the auditor's responsibility for fraud detection in both an IT and non-IT setting. A variety of differing risk assessment methods is examined.

Chapter 4 explores in detail the ISACA Code of Professional Ethics and the current ISACA IS Auditing Standards and Guidelines Standards and discusses the IIA Code of Ethics, Standards for the Professional Practice of Internal Auditing, and Practice Advisories. In addition, standards and guidelines other than the ISACA and IIA models are explored.

Chapter 5 introduces the concepts of corporate governance with particular attention to the implications within an IT environment and the impact on IS auditors. Criteria of Control (COCO), Committee of Sponsoring Organizations of the Treadway Commission (COSO), King, Sarbanes-Oxley Act of 2002, and other recent legislative impacts are examined together with the structuring of controls to achieve conformity to these structures. Control classifications are examined in detail together with both general and application controls. Particular attention is paid to COBIT (Control Objectives for Information and Related Technology) from both a structural and relevance perspective.

Chapter 6 introduces the concept of computer risks and exposures and includes the development of an understanding of the major types of risks faced by the IT function including the sources of such risk as well as the causes. It also emphasizes management's role in adopting a risk position, which itself necessitates a knowledge of the acceptable management responses to computer risks. One of the most fundamental influencing factors in IT auditing is the issue of corporate risk. This chapter examines risk and its nature within the corporate environment and looks at the internal audit need for the appropriate risk analysis to enable risk-based auditing as an integrated approach. This includes the effect of computer risks, the common risk factors, and the elements required to complete a computer risk analysis.

Chapter 7 examines the audit planning process at both a strategic and tactical level. The use of risk-based auditing and risk-assessment methods and standards are covered. The preliminary evaluation of internal controls via the appropriate information-gathering and control-evaluation techniques as a fundamental component of the audit plan and the design of the audit plan to achieve a variety of audit scopes is detailed.

Chapter 8 looks at audit management and its resource allocation and prioritization in the planning and execution of assignments. The management of IS Audit quality through techniques such as peer reviews and best-practice identification is explored. The human aspects of management in the forms of career development and career path planning, performance assessment, counseling, and feedback as well as professional development through certifications, professional involvement, and training (both internal and external) are reviewed.

Chapter 9 exposes the fundamental audit evidence process and the gathering of evidence that may be deemed sufficient, reliable, relevant, and useful. Evidence-gathering

techniques such as observation, inquiry, interviewing, and testing are examined and the techniques of compliance versus substantive testing are contrasted. The complex area of statistical and non-statistical sampling techniques and the design and selection of samples and evaluation of sample results is examined. The essential techniques of computer assisted audit techniques (CAATs) are covered and a case study using the software provided is detailed.

Chapter 10 covers audit reporting and follow-up. The form and content of an audit report are detailed and its purpose, structure, content, and style as dictated by the desired effect on its intended recipient for a variety of types of opinion are considered as well as the follow-up to determine management's actions to implement recommendations.

Part II: Information Technology Governance

This part details the processes involved in planning and managing the IT function and the management issues faced in a modern IT department. The techniques used by management and the support tools and frameworks are examined with respect to the need for control within the processes.

Chapter 11 covers IT project-management, risk management including economic, social, cultural, and technology risk management as well as software quality-control management, the management of IT infrastructure, alternative IT architectures and configuration, and the management of IT delivery (operations) and support (maintenance). Performance measurement and reporting and the IT balanced scorecard are also covered as are the use of outsourcing, the implementation of IT quality assurance, and the socio-technical and cultural approach to management.

Chapter 12 examines IT strategic planning and looks at competitive strategies and business intelligence and their link to corporate strategy. These, in turn, influence the development of strategic information systems frameworks and applications. Strategic planning also includes the management of IT human resources, employee policies, agreements, contracts, segregation of duties within IT, and the implementation of effective IT training and education.

Chapter 13 looks at the broader IS/IT management issues including the legal issues relating to the introduction of IT to the enterprise; intellectual property issues in cyberspace: trademarks, copyrights, patents as well as ethical issues; rights to privacy; and the implementation of effective IT governance.

Chapter 14 introduces the need for support tools and frameworks such as COBIT: Management Guidelines, a framework for IT/IS managers and COBIT: Audit's Use in Support of the Business Support Cycle. International standards and good practices such as ISO17799, IT Infrastructure Library®(ITIL®), privacy standards, COSO, COCO, Cadbury, King, and Sarbanes-Oxley also play a vital role in ensuring the appropriate governance.

Chapter 15 covers the need for, and use of, techniques such as change control reviews, operational reviews, and ISO 9000 reviews.

Part III: Systems and Infrastructure Lifecycle Management

IT is essential to an organization only in so far as it can effectively assist in the achievement of the business objectives. This means that the business-application systems need

to be appropriate to the business needs and meet the objectives of the users in an effective and efficient manner. Part III explores the manner in which application systems are planned, acquired externally, or developed internally and ultimately implemented and maintained. In all cases such systems have an objective of being auditable in addition to the other unique business objectives. This part also examines the variety of roles that the auditor could be called on to undertake and the circumstances and controls appropriate to each.

Chapter 16 covers the IT planning and managing components and includes developing an understanding of stakeholders and their requirements together with IT stay planning methods such as system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment, object-oriented systems analysis, and design. Enterprise Resource Planning (ERP) software to facilitate enterprise applications integration is reviewed.

Chapter 17 covers the areas of information management and usage monitoring. Measurement criteria such as evaluating service level performance against service-level agreements, quality of service, availability, response time, security and controls, processing integrity, and privacy are examined. The analysis, evaluation, and design information together with data and application architecture are evaluated as tools for the auditor.

Chapter 18 investigates the development, acquisition, and maintenance of information systems through Information Systems' project management involving the planning, organization, human resource deployment, project control, monitoring, and execution of the project plan. The traditional methods for the system development life cycle (SDLC) (analysis, evaluation, and design of an entity's SDLC phases and tasks) are examined, as are alternative approaches for system development such as the use of software packages, prototyping, business process reengineering, or computer-aided software engineering (CASE). In addition system maintenance and change-control procedures for system changes together with tools to assess risk and control issues and to aid the analysis and evaluation of project characteristics and risks are discussed.

Chapter 19 examines the impact of IT on the business processes and solutions, business process outsourcing (BPO), and applications of e-business issues and trends.

Chapter 20 looks at the software-development-design process itself and covers the separation of specification and implementation in programming, requirements specification methodologies, and technical process design. In addition database creation and manipulation, principles of good screen and report design, and program language alignment are covered.

Chapter 21 looks at the audit and control of purchased packages to introduce readers to those elements critical to the decision taken to make or buy software. This includes a knowledge of the systems-development process and an understanding of the user's role in training required so that the outsource decision on the factors surrounding it may be made to best effect.

Chapter 22 looks at the auditor's role in feasibility studies and conversions. These are perhaps the most critical areas of systems implementation, and audit involvement should be compulsory.

Chapter 23 looks at the audit and development of application-level controls including input/origination controls, processing control procedures, output controls, application system documentation, and the appropriate use of audit trails.

Part IV: Information Technology Service Delivery and Support

This part examines the technical infrastructure in a variety of environments and the influence the infrastructure has on the management and control procedures required to attain the business objectives. The nature and methodologies of service center management are exposed for discussion.

Chapter 24 examines the complex area of the IS/IT technical infrastructure (planning, implementation, and operational practices). IT architecture/standards over hardware including mainframe, minicomputers, client-servers, routers, switches, communications, and PCs as well as software including operating systems, utility software, and database systems are revealed. Network components including communications equipment and services rendered to provide networks, network-related hardware, network-related software, and the use of service providers are covered as are security/testing and validation, performance monitoring, and evaluation tools and IT control monitoring and evaluation tools, such as access control systems monitoring and intrusion-detection-systems monitoring tools. In addition, the role of managing information resources and information infrastructure through enterprise management software and the implementation of service center management and operations standards/guidelines within COBIT, ITIL, and ISO 17799 together with the issues and considerations of service center versus proprietary technical infrastructures are explored.

Chapter 25 introduces the areas of service center management and the maintenance of Information Systems and technical infrastructures. These involve the use of appropriate tools designed to control the introduction of new and changed products into the service center environment and include such aspects as security management, resource/configuration management, and problem and incident management. In addition, the administration of release and versions of automated systems as well as the achievement of service-level management through capacity planning and management of the distribution of automated systems and contingency/backup and recovery management are examined.

The key management principles involved in management of operations of the infrastructure (central and distributed), network management, and risk management are outlined as are both the need for customer liaison as well as the management of suppliers.

Part V: Protection of Information Assets

This part examines the essential area of IT security in all of its manifestations. The administration of security focusing on information as an asset is commonly problematic and may frequently be observed as a patchwork of physical and logical security techniques with little thought to the application and implementation of an integrated approach designed to lead to the achievement of specific control objectives.

Chapter 26 looks at the area of information assets security management. This covers information technology and security basics and the fundamental concepts of IT security. The need for securing IT resources and maintaining an adequate policy framework on IT asset security, the management of IT security, and security training standards are examined as are the major compliance and assurance issues in IT security.

Chapter 27 covers the critical area of the components of logical IT security. Logical access control issues and exposures are explored together with access-control software. The auditing of logical access to ensure the adequate control of logical security risks using the appropriate logical security features, tools, and procedures is detailed.

Chapter 28 looks at the application of IT security including communications and network security. The principles of network security, client-server, Internet and web-based services, and firewall security systems are all detailed together with connectivity protection resources such as cryptography, digital signatures, digital certificates, and key management policies. IT security also encompasses the use of intrusion-detection systems and the proper implementation of mainframe security facilities. Security is also a critical element in the development of application systems and involves both the systems development and maintenance processes and database design.

Chapter 29 examines the concepts of physical IT security including physical access exposures and controls.

Part VI: Business Continuity and Disaster Recovery

In many organizations, the ongoing continuity and availability of an information-processing capability is critical to the corporate survival of the entity. This part explores the need for and techniques utilized in the protection of the information technology architecture and assets through both disaster recovery planning and the transfer of risk by utilizing the appropriate insurance profile. The auditor's role in examining corporate continuity plans is examined in detail.

Chapter 30 introduces the activities required to ensure the protection of the IT architecture and assets. These include backup provisions involving business-impact analysis and business-continuity planning leading to IT disaster recovery planning, obtaining management support and commitment to the process, plan preparation and documentation, obtaining management approval, and distribution of the plan. In addition, the testing, maintenance, and revision of the plan together with audit's role in all of these activities are investigated.

Chapter 31 looks at insurance and the variety of insurance coverage that can be obtained. Issues such as the valuation of assets, including equipment, people, information processes, and technology, are examined.

Part VII: Advanced IT Auditing

The final part explores the technical auditor's function and role in auditing specialized areas such as the audit and control of e-commerce systems, auditing operating systems at both micro and mainframe levels, securing systems against outside penetration, and investigating security breaches.

Chapter 32 examines the tasks required to establish and optimize the IT audit functions including defining the scope of IP auditing, setting the objectives, staffing, and training. Measuring the effectiveness of the IT audit and the role of the specialist are critical in producing an effective IT audit function. It also introduces readers to the concepts of the paperless society inherent in e-commerce, business-2-business (B2B), business-2-consumer (B2C), and electronic data interchange (EDI) in general. These concepts change the internal control structure required in such an environment as well as changing the sources of what audit and legal evidence is available. The auditor will be required to implement the correct program to bring the contoured auction in line with this changing business environment.

Chapter 33 takes the reader through the advanced concepts of auditing within a UNIX / Linux environment including the major threat categories and control opportunities as well as the use of the appropriate audit tools.

Chapter 34 covers in detail the theory and practice of auditing within a Windows Vista or Windows 7 environment. This again includes the major control opportunities, controls to be sought, and audit tools to be used.

Chapter 35 addresses the major risk of computer hackers including definitions of how hackers gain entrance and the design of the appropriate security hierarchy in order to effectively manage this critical risk.

Chapter 36 examines the problem of computer fraud and countermeasures to prevent, detect, and alleviate the problems. This includes the effect of the risk of fraud on the business control objectives, the techniques applicable for determining higher risk, as well as the impact of computer fraud on an organization. The ability to distinguish between types of computer fraud, and the nature and effect as well as identification of likely fraud indicators enables the structuring of an appropriate antifraud security environment. The auditor must be capable of distinguishing between fraud and forensic auditing and applying the appropriate techniques. This involves an understanding of the rules that influence the acceptability of computer evidence as legally acceptable and binding evidence.

Appendices

Five appendices will be found at the back of the book including the appropriate ethics and standards for the IT auditor as well as sample audit programs for:

- Application Systems Auditing
- Logical access control
- UNIX / Linux environments
- Windows Vista and Version 7

Auditor's Guide to IT Auditing

