IT AUDIT, CONTROL, AND SECURITY

ROBERT R. MOELLER

IT Audit, Control, and Security

ROBERT MOELLER

WILEY
John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Moeller, Robert R.

IT audit, control, and security / Robert Moeller.

p. cm.

Includes bibliographical references and index.

ISBN: 978-0-471-40676-1 (cloth); 978-0-470-87741-8 (ebk); 978-0-470-87767-8 (ebk); 978-0-470-87768-5 (ebk)

1. Information technology—Auditing. 2. Electronic data processing departments—Auditing. 3. Computer security. 4. Computer networks—Security measures. I. Title.

T58.5.M645 2010

658.4'78–dc22 2010013505

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Introduction: Importance of IT Auditing

WELCOME TO THE WORLD of *IT Audit, Control, and Security.* Much has changed in information technology (IT) auditing since we published our first edition of this book when we were then called *Computer Auditors.* Back in those days, traditional mainframe or legacy computer systems were still common, we had difficulty envisioning laptop systems as serious business information systems tools, and the Internet was little more than an e-mail and text document communications tool for many. Computer security then was largely based on locked, secured mainframe facilities, and we were just seeing the very first computer viruses. Many auditors, both internal and external, typically had only limited knowledge about IT systems controls, and there were wide knowledge gaps among auditors, systems security specialists, and developers. It is hard to focus on just one development or event that has turned our view of IT audit controls into a separate discipline. However, the overall influence of the Web along with audit, security, and internal controls concerns has made IT controls more important to many today.

This book focuses on both the technical and professional issues facing today's audit, security, and internal control specialists in an information systems environment, with the goal of providing an understanding of key IT audit security and internal controls issues. We have expanded our audience beyond just auditors to include IT security and internal control specialists as well. Although some may not have not have specific job titles covering these audit, security, and internal controls disciplines, many professionals in today's enterprises have a responsibility to ensure that good IT controls have been installed and are operating. IT auditors are key persons responsible for assessing these controls. Although the individual chapters of this book, outlined next, cover a broad range of technical and audit-related topics, each of the chapters focuses on three broad IT audit topic areas:

1. Technology-driven audit and internal controls. The effective IT auditor today needs to have a good understanding of a wide range of IT technologies as well as appropriate related audit, security, and control issues and techniques. As our first broad concentration area, the text addresses some of the more significant technology changes today along with their audit, security, and internal control implications. This book is not a detailed technology tutorial, but we describe important IT issues and introduce their IT control procedures in the following broad areas:

- Electronic commerce systems, including the use of the XBRL protocol as well as wireless and cloud computing. This area generally goes under the name of "e-business" with evolving standards and good practices.

- Modern application implementation processes, including the use of comprehensive enterprise resource planning (ERP) software packages, software as a service (SAAS) implementation approaches and object oriented-application development processes.
- Effective IT continuity planning processes. Because virtually all enterprise operations today are tied to often interlocking IT processes, facilities must be in place to restore them to normal operations if some unexpected event arises.
- Systems infrastructure controls for managing existing applications and operations. Configuration management, service-level agreements, and effective customer service functions are all important in today's modern IT environment.
- Effective IT governance procedures. Whether Sarbanes-Oxley Act (SOx) rules or international standards guidelines, all IT organizations today must understand and comply with the many new rules covering all aspects of IT governance and operations.
- The importance of storage management. Effective processing rules and IT governance requirements require that we keep backup copies of much of the data we use in IT operations as well as database operations to allow an enterprise to search for and retrieve that data easily. IT storage audit, security and internal control issues, and newer concepts such as virtualization are important IT concerns.
- Modern computer security procedures, including trusted networks and firewall-protected systems. Enterprises need to protect their data in light of ever-increasing threats in today's Web and wireless environments.

This list is not all-encompassing but highlights the overall topics in these chapters. Although some of these expressions may seem like buzzwords or techno-jargon to some readers, the chapters to come introduce many technical concepts with an emphasis on their related audit, security, and internal control concepts and procedures.

2. Security, privacy, and continuity issues. As the second broad topic area in this book, we discuss disaster recovery planning as well as effective continuity and information systems security processes in a modern IT environment. The emphasis is more on getting the business back in operation rather than just getting the IT resources working again. Closely related to security matters, privacy is another issue facing IT auditors. We are increasingly seeing legislation mandating privacy protections over multiple types of information systems data, such as medical records, financial data, and other areas. These new rules have encouraged many enterprises to install strengthened internal controls.

3. Auditing legislative and governance changes. Professionals constantly face legal and other changes that impact their work. Understanding and developing appropriate procedures is this book's third broad objective. Although it occurred years ago now, the catastrophic failure of the then-prominent corporation, Enron, introduced a raft of new issues. Based on its stock market capitalization, Enron was then a rapidly growing large company engaged in trading oil, gas, and other commodities. Enron's financial reports, in retrospect, contained many red-flag warnings of possible troubles. Despite these warning signs, Enron's external auditors seemingly looked the other way.

Enron subsequently collapsed, hurting many and leaving a trail of recriminations and questions about the overall independence and objectivity of its external auditors. As a result, the U.S. Congress passed the Sarbanes-Oxley Act (SOx), which changed the

process of auditing internal accounting controls for financial management as well as for external and internal auditors. The text discusses how SOx rules continue to impact auditors and financial management with a focus on internal controls, security, and IT auditing.

The worldwide market meltdown starting in 2008 has caused a series of other concerns when what were then major financial and other enterprises worldwide either totally failed or lost value to investors. Audit, security, and internal control issues and concerns do not just arise because of a single event, such as the 9/11 terrorism attack or the Enron bankruptcy. Our third focus area, auditing legal and governance changes, evolves over time, and we will discuss newer issues and what we feel are evolving concerns. Our emphasis over these next chapters is on newer rules, evolving technologies, and their combined impact on today's IT audit professional.

Our text covers a blend of audit, internal control, and security issues that are key knowledge areas for IT auditors. These are also topics where financial (often external) auditors, internal audit management, and other professionals who are not IT audit specialists should have at least some general understanding. IT security and controls issues have become so pervasive today that enterprise professionals at many levels should have a general knowledge of them.

An overall objective of this book is to highlight areas that are the most important, from an internal controls risk perspective, for today's IT auditors. These chapters present a high-level overview of each of the three broad objective areas just discussed. No matter what the technical topic, there are always opportunities to present even more detailed technical information. However, we focus on areas that we feel are important to today's professional, whether an enterprise IT audit staff member, a manager, or a student learning more. In summary, the chapter-by-chapter IT audit, control, and security topics discussed in this book include:

Chapter 1, SOx and the COSO Internal Controls Framework. The Sarbanes-Oxley Act and its internal controls assessment rules have been the biggest regulatory changes in decades, and they have impacted both auditors and enterprise management in the United States and worldwide. This chapter summarizes the SOx Section 404 requirements for internal control reviews to support an enterprise's financial reports. Our emphasis, however, is on internal accounting controls reviews of primarily IT applications. The chapter also discusses the newer financial audit AS5 rules released in late 2008.

In addition, we discuss the Committee of Sponsoring Organizations (COSO) framework on internal controls as well as some the newly released COSO guidance materials for monitoring internal control systems. This chapter emphasizes an IT auditor's responsibility for understanding and using the COSO internal controls framework.

Chapter 2, Using CobiT to Perform IT Audits. A more IT-oriented internal controls framework, called Control *Ob*jectives for *I*nformation and related *T*echnology (CobiT), was in place even before SOx, and many enterprises began to use CobiT when SOx became the law as a preferred tool for complying with its Section 404 internal controls procedures. The CobiT framework provides guidance on evaluating and understanding internal controls, with an emphasis on enterprise IT resources. CobiT is not a replacement for the COSO internal controls framework but is a different way to look at internal controls in today's IT-centric world.

Although originally launched as a tool to help specialist internal and external auditors who reviewed IT-related internal controls, CobiT today is a helpful tool for evaluating all internal controls across an enterprise. It emphasizes the linkage of IT with other business resources to deliver overall value to an enterprise. This chapter provides an overview of the CobiT framework and its key components. More important, the chapter describes the relationship between CobiT objectives and the COSO internal control framework for use in internal audit reviews. Even if an internal auditor does not use the CobiT framework in reviews of internal controls, all internal and IT auditors should have a high-level knowledge of the basic CobiT framework. Knowledge of CobiT and the COSO internal controls framework will help an IT auditor to better understand the role of IT controls and risks in many enterprise environments.

Chapter 3, IIA and ISACA Standards for the Professional Practice of Internal Auditing. Every profession requires a set of standards to govern their practices, general procedures, and ethics. The key standards for all internal auditors are the Institute of Internal Auditors' (IIA's) Professional Standards for the Practice of Internal Auditing, a set of guidance materials that were most recently revised in 2009. This chapter summarizes the current IIA standards and provides guidance on how to apply them. The chapter also introduces the IIA's Global Technology Audit Guide (GTAG) series IT guidance materials. An understanding of the IIA's International Standards is an absolute must for all internal and IT auditors. These standards provide the support for many if not nearly all internal audit professional activities.

This chapter also revisits the IIA Code of Ethics, an important supporting foundation for internal and IT auditors, as well as the Code of Ethics for the Information Systems Audit and Control Association (ISACA). ISACA members are often IIA members or Certified Public Accountants, but the ISACA Code of Ethics places a special emphasis on IT-related activities. Although ISACA does not have the same type of standards as the IIA, its CobiT IT internal control framework provides standards guidance for IT auditors. The chapter also highlights ISACA's standards and guidelines. These are particularly important for IT auditors.

In addition, Chapter 31 introduces another very important set of internal audit standards, the quality audit standards from the American Society for Quality (ASQ). ASQ's internal audit standards and its quality auditors represent a different dimension and discipline when contrasted with the IIA's and ISACA's approaches and standards. They also represent an area that must be better represented and understood in the overall world of internal auditing.

Chapter 4, Understanding Risk Management through COSO ERM. Although the term *enterprise risk management* (ERM) is frequently used, many IT auditors do not have a consistent understanding of and how to use it as a tool for effective internal audit reviews. This chapter introduces the COSO Enterprise Risk Management (COSO ERM) framework and its elements. Although their basic framework models look similar, COSO ERM is different from the COSO internal controls framework discussed in Chapter 1. COSO ERM is an important reference to better understand and evaluate the risks surrounding internal controls at all levels. This chapter describes the major elements of the COSO ERM framework and looks at how IT auditors can better build

COSO ERM into their review processes as well as steps for auditing the effectiveness of an enterprise's risk management processes.

Every IT auditor needs to have an understanding of risk assessment approaches and the overall risk management process, with an emphasis on COSO ERM. This chapter presents IT audit techniques for understanding and assessing risks in many areas, from selecting items to review to evaluating risks as part of IT audit reviews.

Chapter 5, Performing Effective IT Audits. This chapter describes basic processes for performing an effective IT audit. Basic reviews can be performed by many specialists in an enterprise, but this chapter focuses on basic audit steps for performing an IT internal audit review, ranging from risk-based audit planning to preparing effective internal audit reports.

This chapter does not describe the overall internal audit review process but emphasizes some of the key elements necessary to perform effective IT-related reviews.

Chapter 6, General Controls in Today's IT Environments. IT processes and systems today range from an application to control an enterprise's accounting general ledger to the all-pervasive Internet. Although the lines of separation are sometimes difficult, we can generally think of IT controls on two broad levels: application controls that cover a specific process—such as an accounts payable application to pay invoices from purchases—and what are called general IT controls. This latter category covers internal controls that do not relate just to specific IT applications but are important for all aspects of an enterprise's IT operations.

The concept of IT general controls goes back to the early days of centralized, mainframe computers. At that time, internal auditors sometimes looked for such things as an access control lock on a computer center door as a general control that covered all processes and applications operating from within the centralized IT operations center. Today, we often think of the processes that cover all enterprise IT operations as the IT infrastructure, a concept further discussed in Chapter 7.

This chapter discusses reviews of IT general controls from an IIA standards and CobiT perspective. Although general controls were once considered in terms of centralized mainframe computer center operations in an earlier era, today we should think of them as those controls impacting any set of similar IT machine resources. For example, an internal audit function may equip its entire staff with laptop computers, and good general controls are necessary in this environment to encourage all internal and IT auditors to use common software control procedures on those assigned laptops. General controls weaknesses can impact all IT processes.

Chapter 7, Infrastructure Controls and ITIL Service Management Best Practices. This chapter looks at IT general controls based on the worldwide recognized set of best or good practices called the Information Technology Infrastructure Library (ITIL). These ITIL recommended best practices outline the type of framework an IT auditor should consider when reviewing IT internal control risks and recommending effective IT general controls improvements.

ITIL processes cover what we frequently call the IT infrastructure—the supporting processes that allow IT applications to function and deliver their results to systems users. For example, an ITIL process outlines best practices for installing an effective IT help desk operation for all systems users. All too often, auditors have focused their attention

on the application development side of IT and ignored important service delivery and support IT processes. An enterprise can put massive efforts into building and implementing a new budget forecasting system, but that application will be of little value unless there are good problem and incident management processes in place to allow the users of this budget forecasting system to resolve systems difficulties. Also needed are good capacity and availability processes to allow the new application to run as expected. ITIL processes are part of what is called the IT infrastructure. IT auditors should have a good understanding of these enterprise processes, and they should be covered in IT audit general controls reviews.

Chapter 8, Systems Software and IT Operations General Controls. Whether it is a Microsoft Windows operating system on a laptop computer or Linux controlling an office server, the operating system (OS) and its supporting software are key components to any computer system operation. This chapter discusses some of the various OS types and the supporting systems software that are essential in an IT operation. IT auditors should have a very general understanding of the purposes and importance of these types of IT software and should look for effective general controls when performing reviews in this important general controls area.

Chapter 9, Evolving Control Issues: Wireless Networks, Cloud Computing, and Virtualization. New IT technologies make many processes easier to use or more efficient, but they often introduce new internal control concerns. This chapter has selected three of these newer areas and considers internal control risks and potential audit procedures for each. Wireless networks is the first topic here. Although it is certainly convenient to not have to connect IT terminals and other devices through a formal cable network, the very open environment of using wireless technology approaches introduces some security and control risks. The chapter looks at wireless networks from an audit, security, and control perspective.

As a second topic area, the chapter introduces the rapidly evolving IT configuration called cloud computing. Although the term sounds almost exotic to many, it has become a significant concept today with our growing dependence on using Web-based applications for many business processes rather than applications downloaded to home office servers. Cloud computing processes are also called web services, software as a service (SaaS), or service-oriented architecture (SOA). In cloud computing, many different Internet applications—supported by multiple vendors and operating on multiple servers—operate together out of what looks like a large fuzzy Internet cloud. This chapter introduces cloud computing concepts and discusses some security and controls concerns that may impact IT auditors in their assessments of IT general controls.

This chapter's third topic is virtualization. With the massive amount of data and information that most enterprises retain, storage management is very important for almost all IT operations. Whether it is the very high-capacity miniature USB devices so common today or new database tools, there is a need to install appropriate controls in these storage management environments. In virtualization, any device can be defined to look like another. This concept can create a challenging environment for an IT auditor, and the chapter provides some introductory internal controls guidance to these evolving areas.

Chapter 10, Selecting, Testing, and Auditing IT Applications. In order to perform internal controls reviews in specific areas of enterprise operations, such as accounting, distribution, or engineering, IT auditors must have the skills to understand, evaluate, and test the controls over their supporting IT applications. Reviews of specific application controls often are more critical to achieving overall audit objectives than reviews of general IT controls.

This chapter discusses approaches to review internal accounting controls in IT applications, using several different types of applications as examples. The chapter also discusses audit approaches for evaluating and testing those application controls as well as techniques for reviewing new applications under development. We focus on the internal control characteristics of different types of applications and then discuss how to select appropriate applications in internal controls reviews. There are many differences from one application to another; this chapter focuses on how an IT auditor should select higher-risk applications as candidates for IT audit reviews; the tools and skills needed to understand and document application internal controls; and, finally, processes to test and evaluate those applications.

Chapter 11, Software Engineering and CMMi. The Carnegie-Mellon University Software Engineering Institute's IT-based Capability Maturity Model for integration (CMMi®) is an effective approach for an enterprise and its IT software development functions to assess how well they are organized. It is a measure on whether processes are well managed, repeatable, or even unpredictable. IT auditors can use CMMi as a tool to measure how well they are doing, and it can serve as a guide for process improvements. The chapter provides an overview of how IT audit specialists can use CMMi in their assessments of internal controls and in organizing their own IT projects.

Chapter 12, Auditing Service-Oriented Architecture and Record Management Processes. SOA is an IT systems approach where an application's business logic or individual functions are modularized and presented as services for consumer/client applications. This chapter introduces SOA concepts for the IT auditor and discusses internal control and IT auditor issues surrounding the development and operations of IT applications using this technology. The chapter also reviews the importance of effective records management systems in today's enterprises from an internal controls and IT audit perspective. Today, almost all business records are created and most live their entire lives electronically. Failure to manage electronic records and physical records in accordance with established records management principles ignores potential risk.

Chapter 13, Computer-Assisted Audit Tools and Techniques. IT auditors test and review the internal controls surrounding their IT systems, and they often need tools to better understand and evaluate the completeness and accuracy of the data stored in the IT applications' files and databases. This chapter reviews approaches to retrieving data through computer-assisted audit tools and techniques (CAATTs), the use of independent auditor–controlled software to assess organization IT files and documents. Whether purchased software administered by an IT auditor or an operational procedure to better analyze IT data, many tools and techniques can help make audit reviews of IT-supported systems more efficient and effective. The chapter provides IT auditors with a basic understanding on the general use of CAATTs to access and review automated data to support IT audits.

Chapter 14, Continuous Assurance Auditing, OLAP, and XBRL. Continuous assurance auditing (CAA) is the process of installing control-related monitors in automated systems such that these monitors will send messages to internal auditors if the system's processing signals a deviation from an established audit limit or parameter. This chapter discusses CAA as an improved alternative approach for reviewing automated systems as well as an overview of continuous monitoring (CM), business controlled procedures that can be subject to periodic internal IT audits.

The chapter also introduces XBRL, the *e*xtensible *b*usiness *r*eporting *l*anguage developed by the American Institute of Certified Public Accountants. XBRL is a standards-based way to communicate business and financial information across multiple enterprises. IT auditors should have a basic understanding of XBRL, a methodology that is growing in recognition and use, and its necessary supporting internal controls.

Chapter 15, IT Controls and the Audit Committee. The management or supervisory authority of enterprise's internal audit function is the board of directors' audit committee. This committee is responsible for approving internal audit plans, reviewing audit reports, hiring internal audit management, and taking other actions as appropriate. Although historically much of an audit committee's interests have been based on audited financial statements and an enterprise's financial audit, IT audit has an important role here as well. This chapter examines planning and reporting key IT audit activities to the enterprise's audit committee.

Chapter 16, Val IT, Portfolio Management, and Project Management. This chapter looks at three knowledge areas that are important to IT auditors: (1) ISACA's enterprise value initiative, called Val IT, to better manage and understand IT investments; (2) portfolio management approaches to better deal with the large number of diverse applications and IT resources in the typical enterprise; and (3) project management good practices to better control and manage many IT activities. Internal audit functions normally should develop an audit universe list, a compilation of all potential auditable entities for that enterprise. The chapter also looks at audit universe portfolio management from an IT audit perspective.

The chapter also discusses the importance of effective project management procedures. Audits and internal control activities should be planned and performed in a well-organized manner. The program and project management procedures described in the chapter will aid in this process.

Chapter 17, Compliance with IT-Related Laws and Regulations. Both in the United States and worldwide, a wide range of laws and regulations impact enterprise IT operations. Some of these have direct IT connections, such as the U.S. Computer Fraud and Abuse Act (CFAA), while others, such as SOx, are not really IT-related laws but nevertheless have multiple IT relationships. This chapter reviews a series of primarily U. S. IT-related laws and regulations, highlighting areas that should be considered in IT audit reviews.

Chapter 18, Understanding and Reviewing Compliance with ISO Standards. The International Standards Organization (ISO) has guidance that covers a wide range of areas, such as defining fastener screw threads in an automobile engine, the thickness of a personal credit card, and IT quality standards. This chapter provides an overview and introduction to several of the many ISO standards that are particularly

important for IT auditors, with a focus on ISO 27001 and 27002 computer security standards. The chapter also provides an introduction to several other ISO standards, including international standards for IT management systems and for quality management. Enterprise compliance with appropriate ISO standards is important worldwide today, as they establish benchmarks for worldwide compliance.

Chapter 19, Controls to Establish an Effective IT Security Environment. Effective IT security is very important in all enterprises. Beyond password controls and backup processes discussed in other chapters, an enterprise needs a high-level enterprise commitment to IT security as well as strong procedures to build effective IT security processes. These procedures can range from such matters as a strong enterprise code of conduct setting the rules for enterprise associates to overall management policies promoting the need for an effective security environments. This chapter outlines some techniques as well IT audit procedures to review enterprise-wide IT security effectiveness.

Chapter 20, Cybersecurity and Privacy Controls. In our Web-dominated world today, IT security or cybersecurity and privacy controls over data and information are very important. This chapter discusses these controls from two focus areas: (1) some of the many cybersecurity and privacy concerns that IT auditors should consider in their reviews of systems and processes and (2) IT privacy issues. We have limited our focus to only some cybersecurity areas because the field of IT security controls is vast and sometimes very technical, beyond the skills of many auditors. Regarding IT privacy, there is a growing set of issues about how much personal data and information individuals should allow to be given to interested enterprises, government authorities, and even other individuals.

Chapter 21, IT Fraud Detection and Prevention. An effective auditor needs to recognize potential fraudulent business practices as part of any IT audit and then should recommend controls and procedures to limit exposure to the fraudulent activity. This chapter outlines some of the red flags—common conditions that an IT auditor might encounter when faced with a potential fraud as well as steps to identify, test, and properly process fraudulent activities. Fraud investigation can be a very detailed and specialized activity, but IT auditors should have a high level understanding of how to audit for potentially fraudulent activities as well as of processes for investigating and reporting fraud. Fraudulent activities represent a breakdown in a wide range of good practices and procedures, but IT auditors must recognize that fraudulent activities always may exist.

Chapter 22, Identity and Access Management. With all of the personal data stored in so many IT databases and systems, there is always a major concern that some perpetrator will hijack and steal someone's personal information to use for improper purposes. The concern that someone will steal this personal information is called identity management. Although certain laws are in place to prohibit such actions, an enterprise needs to establish strong procedures to discourage such improper activities. Starting with effective IT password access controls and the monitoring of potential password violations, an enterprise needs to have strong identity and access management processing in place. This chapter outlines procedures that are effective for IT security management and provides guidance for performing effective IT audits.

Chapter 23, Establishing Effective IT Disaster Recovery Processes. This chapter introduces what is called IT disaster recovery planning processes. (Chapter 25 discusses business continuity controls, which are similar but very different.) IT disaster recovery includes effective backup processes for restoring all aspects of IT operations, whether a classic server-based data center or a network of laptop or desktop system operations. The chapter briefly introduces some of the technical tools, such as data mirroring, that improve IT disaster recovery procedures today. The chapter concludes with guidance on testing disaster recovery plans as well as steps for auditing such plans. Because of our massive dependence on IT operations, effective disaster recovery plans are key components in IT operations.

Chapter 24, Electronic Archiving and Data Retention. Because so much data and supporting documentation is recorded on databases or other IT media formats, it is important to preserve backup copies in separate, independent locations. This is as true for an enterprise with massive business transactions as it is for an IT auditor. The chapter discusses some best practice approaches for saving and archiving data as well as control procedures for its access. In addition, the chapter outlines steps for an audit of data retention processes.

Chapter 25, Business Continuity Management, BS 25999, and ISO 27001. This chapter introduces best practices for effective enterprise IT continuity and disaster recovery planning processes including establishing enterprise internal controls in enterprise-critical areas. Going beyond Chapter 24's disaster recovery backup procedures, continuity planning is based on the concept that an enterprise needs to have processes in place to resume normal business operations in the event of a major disruption in IT services. This major task involves restoring business process operations beyond just the IT applications.

This chapter also discusses BS 25999, a U.K.-based standard for business continuity management as well as the ISO 27001 international standards. The chapter uses BS 25999 to describe the processes necessary for effective continuity planning for a sample enterprise.

Chapter 26, Auditing Telecommunications and IT Communications Networks. Moving beyond the wireless networks discussed in Chapter 9, enterprise IT systems typically are tied to vast telecommunications networks, internally or through the Web. This chapter provides an introduction to the wide variety of network topologies in place today and outlines processes surrounding IT network controls and tools such as scanners and sniffers. The chapter outlines approaches for an IT auditor's internal controls and security-related review of an enterprise's telecommunications including its wireless operations.

Chapter 27, Change and Patch Management Controls. Enterprises can be exposed to major security vulnerabilities in the event of unauthorized or inappropriate changes to its IT systems and programs. Strong IT change management processes are always needed. This chapter discusses effective IT change and patch management controls and introduces procedures for auditing internal controls in these areas.

Chapter 28, Six Sigma and Lean Technologies. Enterprise operations managers, at all levels, are regularly looking for ways to improve their operations, whether in shop-floor production processes, office administrative procedures, or elsewhere. Many

have found six sigma processes to be effective here. This chapter provides a high-level introduction to six sigma concepts and how they can be applied to enterprise IT operations. We provide an overview of six sigma and the lean approaches to implementing it. Even though an internal or IT audit function may not be using six sigma concepts as part of their overall operations, IT auditors should have a basic understanding of this important quality improvement concept.

Chapter 29, Building an Effective IT Internal Audit Function. Other chapters have discussed many aspects of IT audits. This chapter steps back and looks at some the requirements for an enterprise to build an effective IT audit function as part of their overall internal audit group. The chapter reviews IT audit positions descriptions, audit planning, workpapers, audit reports, and other factors needed to build an effective IT internal audit function.

Chapter 30, Professional Certifications: CISA, CIA, and More. IT auditors have a need for strong and well-recognized professional certifications. Many have joined the profession with no specific certification requirements beyond their undergraduate college degrees; others attained accounting degrees and prepared for the Certified Public Accountant (CPA) examination. Today, an IT auditor can take a qualifying examination and complete other requirements to become a Certified Information Systems Auditor (CISA), a Certified Internal Auditor (CIA), a Certified Fraud Examiner (CFE), or any of a series of other certifications. This chapter discusses the professional designations that are important to the IT auditor, with an emphasis on the CIA and CISA certifications, including their qualification and examination requirements. In addition, the chapter considers some other certification options available to IT auditors, including the Certified Information Systems Security Professional (CISSP) requirements.

Chapter 31, Quality Assurance Auditing and ASQ Standards. This chapter reviews the role of quality auditors in an enterprise, their practices and standards. There are many similarities between the activities of quality auditors and the IT auditors that are the main focus of this book. With a growing convergence of enterprise activities to improve governance, IT processes, and internal controls, we can expect to see these internal audit groups become more closely aligned. Although we focus more on IIA and ISACA types of IT internal auditors, there also is a need for a general understanding of the roles, responsibilities, and activities of quality auditors. In addition, we also consider internal audit Quality Assurance (QA) reviews of an IT audit function performed by members of the internal audit team themselves or by contracted outside reviewers.

HOW TO USE THIS BOOK

The role of an IT auditor is changing now and will change even more in the future. The internal control SOx, COSO, and CobiT models presented in Chapters 1 and 2 suggest a much broader role for the IT audit and internal controls specialist of the future. In addition, technology changes and new concepts, such as many of the newer issues introduced throughout this book, will require that IT auditors develop expanded knowledge needs. An overall objective of this book is to introduce some of these newer

concepts. Our objective is not to provide an exhaustive tutorial in each subject area but to discuss concepts and related IT audit, security, and internal controls issues.

The chapters throughout this book contain many suggested audit programs—the steps necessary to perform actual IT audits. There is an increasing need for persons with a broad knowledge of IT audit, security, and internal controls. Although there is also a need for some with very specialized skills, such as a computer crime investigator or a financial auditor with detailed knowledge of a specialized area, such as bond indentures, today's IT auditor should have good skills in the overall areas of audit, control, and security. Providing an overview and some background guidance is a goal of this edition. The author hopes that this edition and potentially more frequent updates will help to provide both new and experienced audit and internal control specialists with information to help them become more effective professionals.

Contents