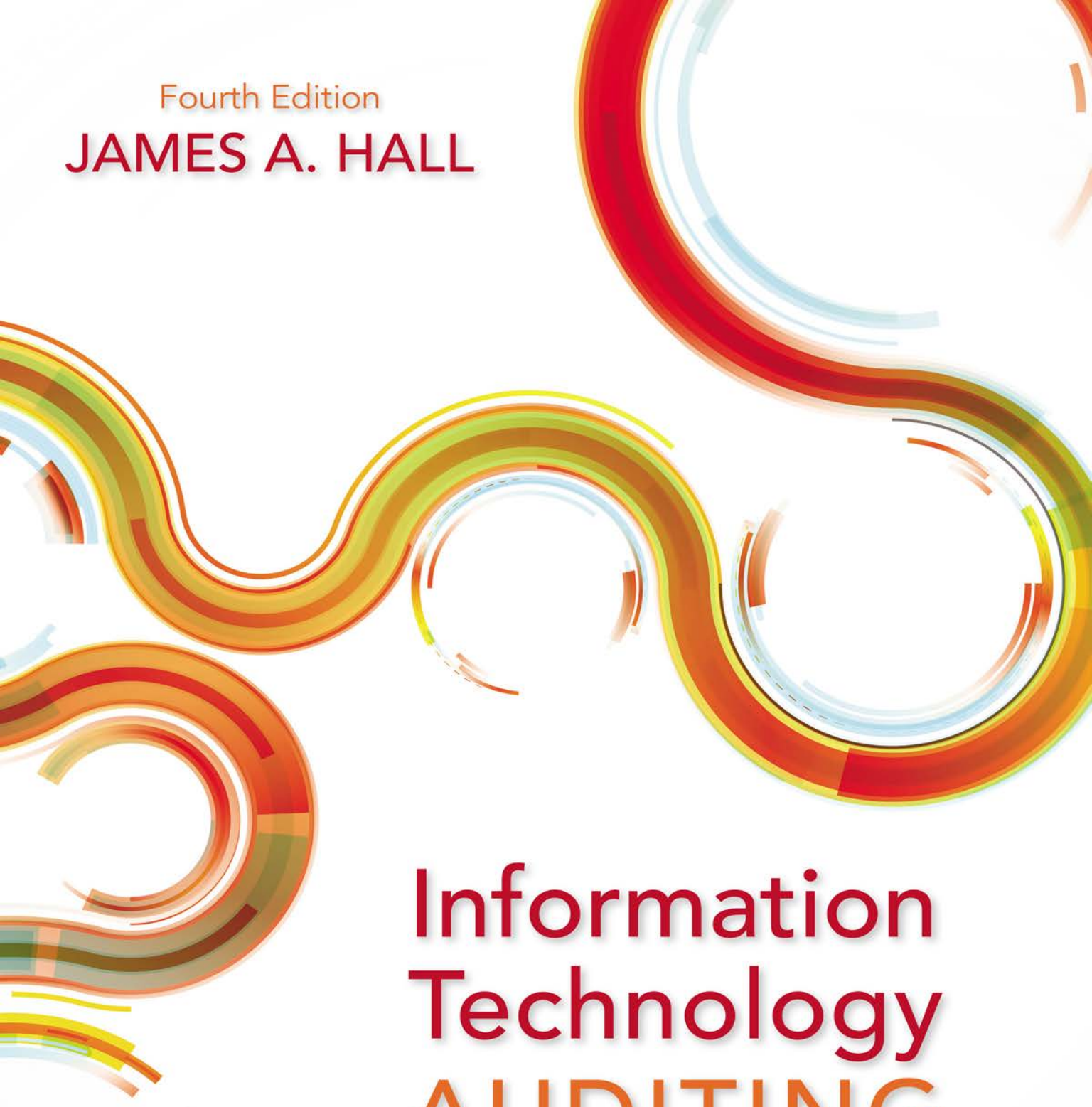
Fourth Edition

JAMES A. HALL



Information Technology AUDITING

INFORMATION TECHNOLOGY AUDITING

FOURTH EDITION

JAMES A. HALL
Lehigh University

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE Learning®

Information Technology Auditing, Fourth Edition

James A. Hall

Vice President, General Manager, Science, Math & Quantitative Business: Balraj Kalsi

Product Director: Mike Schenk

Senior Product Manager: Matthew Filimonov

Content Developer: Theodore Knight

Senior Product Assistant: Adele Scholtz

Marketing Manager: Charisse Darrin

Senior Marketing Coordinator: Eileen Corcoran

Art and Cover Direction, Production Management, and Composition: Lumina Datamatics, Inc.

Intellectual Property

Analyst: Christina Ciaramella

Project Manager: Betsy Hathaway

Manufacturing Planner: Doug Wilke

Cover Image(s): DouDou/Fotolia

Library of Congress Control Number: 2015943916

ISBN: 978-1-133-94988-6

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning Solutions, visit **www.cengage.com**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**

Printed in the United States of America
Print Number: 01 Print Year: 2015

DEDICATION

To my wife Eileen for her unwavering support, encouragement, and patience.

Brief Contents

Contents

Preface

IT AUDITING, 4th edition explores state-of-the-art audit issues to provide students valuable insights into auditing in a modern computer-based environment. The book focuses on the information technology aspects of auditing, including coverage of transaction processing, Sarbanes–Oxley (SOX) implications, audit risk, the Committee of Sponsoring Organizations (COSO) control framework including general and application control issues, fraud techniques and detection, IT outsourcing issues and concerns, and enterprise system risks and controls. Several modules in the text draw upon ACL software. This leading audit tool is supported through projects and cases that are linked to specific chapter topics and provide students with hands-on experience in the use of ACL. Revisions to existing material and the addition of new material in the 4th edition are designed to keep students and instructors as updated as possible on IT auditing issues in an ever-changing technology environment.

DISTINGUISHING FEATURES

A RISK ANALYSIS APPROACH. This text will help the instructor teach a risk-based approach to the identification of key threats and to develop appropriate audit tests and procedures in the following areas: Operating Systems, Data Management, Systems Development, Electronic Commerce (including networks, EDI and Internet risks), Organizational Structure, Computer Center, and Computer Applications (Revenue and Expenditure cycle).

COMPUTER-AIDED AUDIT TOOLS and TECHNIQUES (CAATTs) are frequently used organizations and auditors for testing internal controls and performing substantive tests. This book presents these topics through written text and graphical illustrations to create an easy-to-understand model for student learning. The book also includes numerous assignments and projects that will enable students to develop hands-on expertise in the use of ACL, a leading audit tool.

COMPUTER CONTROL ISSUES and their impact on both operational efficiency and the auditor's attest responsibility are central themes of this textbook. The book contains numerous cases and problems designed to reinforce the learning objectives related to these topics.

STRUCTURED PRESENTATION OF CHAPTER MATERIAL. For clarity and comparability, most chapters are structured along similar lines. They begin with a discussion of the operational features and technologies employed in the area. They then lay out the nature of the risks and explain the controls needed to mitigate such risks. Finally, the chapters define specific audit objectives and present suggested audit procedures to achieve those objectives.

NEW AND REVISED FEATURES

The fourth edition has been rigorously updated to include control and audit issues related to SAS 109, SAS 99, COSO, SSAE 16, and cloud computing. Specific revisions are described next:

End of Chapter Material

The end-of-chapter material in the 4th edition has undergone significant revision. Virtually all multiple-choice question and most of the problems have been revised or replaced. This important body of material is tailored to the chapters' contents, and the solutions provided in the solutions manual accurately reflect the problem requirements. In particular, great attention was paid to internal control and fraud case solutions to ensure consistency in appearance and an accurate reflection of the cases in the text. All case solution flowcharts are numerically coded and cross-referenced to text that explains the internal control issues. This approach, which has been classroom tested, facilitates effective presentation of internal control and fraud case materials.

Updated Chapters 1 through 5

An Updated Chapter 1, Auditing, Assurance, and Internal Control, provides an overview of IT audit issues and auditor responsibilities that follow SOX legislation, the COSO internal control model, and SAS 109. Chapter 2 has been revised to examine audit implications pertaining to Cloud Computing IT outsourcing including virtualization, Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). The new standard for auditing service providers (SSAE 16) is discussed. Chapters 2–5 have been updated to present General Control and audit issues in accordance with SOX and COSO framework

Revised Chapter 8, "Data Structures and CAATTs for Data Extraction"

At one time an accountant in the conduct of an audit could pull an invoice from a filing cabinet. Today that invoice is most likely stored in structured pieces on several normalized database tables and accessing it requires an understanding of relational database structures. The chapter has been extensively rewritten to address this growing need for modern auditors to have a working understanding of data modeling techniques. The chapter presents the key characteristics of the relational database model including data modeling, deriving relational tables from entity relationship (ER) diagrams, the creation of user views, and data normalization techniques.

Revised Chapters 9 "Auditing the Revenue Cycle" and 10 "Auditing the Conversion Cycle"

Chapters 9 and 10 have been extensively revised with new diagrams, flowcharts, and text. Each chapter begins with a review of alternative technologies commonly employed in computer systems. This review is followed by the audit objectives, controls, and tests of controls that an auditor would normally perform. The end of chapter internal control cases have all been revised or replaced.

Updated Chapter 12, Business Ethics, Fraud Schemes, and Fraud Detection

This chapter addresses auditor responsibilities for detecting fraud. It has been revise to include the latest report on occupational fraud and abuse by the Association of Fraud Examiners.

Revised ACL Tutorials

These "how to" tutorials are located on the product Web site and have been revised to be compliant with ACL 9.0. They make it easy for students to quickly understand ACL's extensive capabilities and master its use.

Revised Bradmark ACL Case

To better integrate ACL into the classroom we have revised the Bradmark ACL case, which spans Chapters 9, 10 and 12. This case will enable students to apply many concepts presented in the book using ACL software.

NEW PowerPoint Slides. These downloadable slides, are tightly integrated to the text and contain text page references, exhibits, lecture points, and topic summaries.

ORGANIZATION AND CONTENT

Chapter 1, "Auditing and Internal Control"

This chapter provides an overview of IT auditing. It describes the various types of audits that organizations commission. The chapter distinguishes between the auditor's traditional attestation responsibility and the expanding field of advisory services. It goes on to explain the structure of an IT audit, the relationship between management assertions, audit objectives, tests of controls, and substantive tests. The chapter also outlines the key points of the COSO control framework, which defines internal controls in both manual and IT environments. The final section of the chapter examines audit issues and implications related to SOX legislation and provides a conceptual framework that links general controls, application controls, and financial data integrity. This framework is a model for the remainder of the text.

Chapter 2, "Auditing IT Governance Controls"

This chapter presents the risks, controls, and tests of controls related to IT governance. It opens by definiting IT governance and identifying elements of IT governance that have internal control and financial reporting implications. The topics covered include structuring of the IT function, computer center threats and controls, and disaster recovery planning. The chapter also examines the risks and benefits of IT outsourcing. It concludes with a discussion of audit issues in an outsourcing environment and the role of the SSAE 16 report.

Chapter 3, "Security Part I: Auditing Operating Systems and Networks"

This chapter focuses on SOX compliance regarding the security and control of operating systems, communication networks, Electronic Data Interchange, and PC-based accounting systems. The chapter examines the risks, controls, audit objectives, and audit procedures that may be performed to satisfy either compliance or attest responsibilities.

Chapter 4, "Security Part II: Auditing Database Systems"

The focus of the chapter is on SOX compliance regarding the security and control of organization databases. The chapter opens with a description of flat-file data management, which is used in many older (legacy) systems that are still in operation today. The chapter then presents a conceptual overview of the database model and illustrates how problems associated with the flat-file model are resolved under this approach. The chapter outlines the key functions and defining features of three common database models: the hierarchical, the network, and the relational models. Both centralized and distributed database systems are discussed. The chapter concludes by presenting the risks, audit objectives, and audit procedures relevant to flat files, centralized databases, and distributed database systems.

Chapter 5, "Systems Development and Program Change Activities"

This chapter concludes our treatment of general control issues as they relate to management and auditor responsibilities under SOX Section 404. It begins by describing the roles of the participants involved in developing an organization's information system, including systems professionals, users, and stakeholders. Then it outlines the key activities that constitute the systems development life cycle (SDLC). These include systems planning, systems analysis, conceptual design, system selection, detailed design, system implementation, and program change procedures (systems maintenance). This multistage procedure is used to guide systems development in many organizations. Finally, it discusses SDLC risks, controls, and audit issues.

Chapter 6, "Transaction Processing and Financial Reporting Systems Overview"

This chapter provides an overview of transaction processing systems (TPS) and Financial Reporting Systems (FRS) and presents topics that are common to all TPS and FRS applications. Subsequent chapters draw heavily from this material as we examine the individual systems in detail. The chapter is organized into seven major sections. The first is an overview of transaction processing. This section defines the broad objectives of the three primary transaction cycles and specifies the roles of their individual subsystems. The second section describes the relationship among accounting records in forming an audit trail in both manual and computer-based systems. The third section examines documentation techniques used to represent both manual and computer-based systems. The fourth section reviews the fundamental features of batch and real-time technologies and their implication for transaction processing. The fifth section examines data coding schemes and their role in transaction processing. The sixed section of the chapter illustrates the central role of the general ledger as a hub that connects TPS applications and provides input to the FRS. Finally, the chapter reviews the control and audit issues related to XBRL (extendable business reporting language) initiatives implemented the SEC.

Chapter 7, "Computer-Assisted Audit Tools and Techniques"

Chapter 7 presents the use of Computer-Assisted Audit Tools and Techniques (CAATTs) for performing tests of application controls. The chapter begins with an extensive description of application controls organized into three classes: input controls, process controls, and output controls. It examines both the *black box* (audit around) and *white box* (audit through) approaches to testing application controls. The latter approach requires a detailed understanding of the application's logic. The chapter discusses five CAATT approaches used for testing application logic. These are the *test data method, base case system evaluation, tracing, integrated test facility,* and *parallel simulation*.

Chapter 8, "CAATTs for Data Extraction and Analysis"

Chapter 8 examines the uses of CAATTs for data extractions and analysis. Auditors make extensive use of these tools in gathering accounting data for testing application controls and in performing substantive tests. In an IT environment, the records needed to perform such tests are stored in computer files and databases. Understanding how data are organized and accessed is central to using data extraction tools. For this reason, a thorough review of common flat-file and database structures is provided. Considerable attention is devoted to relational databases, since this is the most common data structure used by modern business organizations. The coverage includes relational concepts, terminology, table-linking techniques, database normalization, and database design procedures.

Data extraction software fall into two general categories: *embedded audit modules* (EAM) and *general audit software* (GAS). The chapter describes the features, advantages, and disadvantages of both. The chapter closes with a review of the key features of ACL, the leading GAS product on the market.

Chapters 9 and 10, "Auditing the Revenue Cycle" and "Auditing the Expenditure Cycle"

Auditing procedures associated with the revenue and expenditure cycles are examined in Chapters 9 and 10 respectively. Each chapter begins with a review of alternative technologies commonly employed in computer systems. This review is followed by the audit objectives, controls, and tests of controls that an auditor would normally perform to gather the evidence needed to limit the scope, timing, and extent of substantive tests. Finally, the substantive tests related to audit objectives are explained and illustrated using ACL software. End-of-chapter material contains several ACL assignments including a comprehensive assignment, which spans Chapters 9, 10 and 12. An appendix to each chapter provides the reader with a detailed description of the activities and procedures that constitute the respective cycle and with the key accounting records and documents employed in transaction processing.

Chapter 11, "Enterprise Reasource Planning Systems"

This chapter presents a number of issues related to the **implementation and audit of enterprise resource planning (ERP) systems**. It is comprised of five major sections.

- The first section outlines the key features of a **generic ERP system** by comparing the function and data storage techniques of a traditional flat-file or database system to that of an ERP.
- The second section describes various ERP configurations related to **servers, databases, and bolt-on software**.
- Data warehousing is the topic of the third section. A **data warehouse** is a relational or multidimensional database that supports online analytical processing (OLAP). A

number of issues are discussed, including data modeling, data extraction from operational databases, data cleansing, data transformation, and loading data into the warehouse.

- The fourth section examines **risks associated with ERP implementation**. These include "big bang" issues, opposition to change within the organization, choosing the wrong ERP model, choosing the wrong consultant, cost overrun issues, and disruptions to operations.
- The fifth section reviews **control and auditing issues related to ERPs**. The discussion follows the COSO control framework and addresses the significant risks associated with role granting activities.

Chapter 12, "Business Ethics, Fraud, and Fraud Detection"

Perhaps no aspect of the independent auditor's role has caused more public and professional concern than the external auditor's responsibility for detecting fraud during an audit. Recent major financial frauds have heightened public awareness of frauds and to the terrible damage it can cause. This chapter examines the closely related subjects of ethics and fraud and their implications for auditing. It begins with a survey of ethical issues that highlight the organization's conflicting responsibilities to its employees, shareholders, customers, and the general public. Management, employees, and auditors need to recognize the implications of new information technologies for such traditional issues as working conditions, the right to privacy, and the potential for fraud. The section concludes with a review of the code of ethics requirements that SOX mandates.

The chapter then considers basic fraud issues beginning with a definition of fraud. The chapter examines the nature and meaning of fraud, differentiates between employee fraud and management fraud, explains fraud-motivating forces, and reviews common fraud techniques. The chapter outlines the key features of SAS 99, "Consideration of Fraud in a Financial Statement Audit," and presents the results of a fraud research project conducted by the Association of Certified Fraud Examiners (ACFE). Finally, the chapter presents a number of specific fraud schemes and fraud detection techniques that are used in practice. The discussion follows the fraud classification format derived by the ACFE, which defines three broad categories of fraud schemes: fraudulent statements, corruption, and asset misappropriation. The chapter presents several ACL tests that auditors can perform to help them detect fraud. The end-of-chapter material contains a number of ACL fraud exercises as well as an integrated fraud case. The fraud assignments and their associated data may be downloaded from this book's Web site.

SUPPLEMENTS

NEW PowerPoint TM slides provide valuable lecture and study aids, charts, lists, definitions, and summaries directly correlated with the text.

The **Solutions Manual**, written by the author, contains answers to all of the end-of-chapter problem material in the text.

The **Product Web site** contains **revised** ACL tutorials, **a revised Bradmark** ACL case, and data files along with instructor solutions. These exercises and cases are tied to chapters in the text.

ACKNOWLEDGMENTS

We wish to thank the following reviewers for their useful and perceptive comments:

Faye Borthick
(Georgia State University)

John Coulter
(Western New England College)

Lori Fuller
(Widener University)

Jongsoo Han
(Rutgers University)

Sharon Huxley
(Teikyo Post University)

Louis Jacoby
(Saginaw Valley State University)

Orlando Katter
(Winthrop University)

Jim Kurtenbach
(Iowa State University)

Nick McGaughey
(San Jose State University)

Rebecca Rosner
(Long Island University—
CW Post Campus)

Hema Rao
(SUNY-Oswego)

Chuck Stanley
(Baylor University)

Tommie Singleton
(University of Alabama at Birmingham)

Brad Tuttle
(University of South Carolina)

Douglas Ziegenfuss
(Old Dominion)

We wish to thank ACL Services, Ltd. for its cooperation in the development of the this and for its permission to reprint screens from the software in the text.

ABOUT THE AUTHOR

James A. Hall is Professor of Accounting, Co-Director of the Computer Science and Business program, and the Peter E. Bennett Chair in Business and Economics at Lehigh University in Bethlehem, PA. After his discharge from the U.S. Army, he entered the University of Tulsa in 1970 and received a BSBA in 1974 and an MBA in 1976. He earned his Ph.D. from Oklahoma State University in 1979. Hall has worked in the field of systems analysis and computer auditing, and has served as consultant in these areas to numerous organizations. Professor Hall has published articles in the *Journal of Accounting, Auditing & Finance*; *Journal of MIS*; Communications of the ACM; *Journal of Management Systems*; Management Accounting; *Journal of Computer Information Systems*; *The Journal of Accounting Education*; The Review of Accounting Information Systems; and other professional journals. He is the author of Accounting Information Systems, 9th edition, published by South-Western College Publishing. His research interests include internal controls, computer fraud, and IT outsourcing.

CHAPTER 1

Auditing and Internal Control

LEARNING OBJECTIVES

After studying this chapter, you should:

- Know the difference between attest services and advisory services and be able to explain the relationship between the two.
- Understand the structure of an audit and have a firm grasp of the conceptual elements of the audit process.
- Understand internal control categories presented in the COSO framework.
- Be familiar with the key features of Section 302 and 404 of the Sarbanes–Oxley Act.
- Understand the relationship between general controls, application controls, and financial data integrity.

Developments in **information technology (IT)** have had a tremendous impact on the field of **auditing**. IT has inspired the reengineering of traditional business processes to promote more efficient operations and to improve communications within the entity and between the entity and its customers and suppliers. These advances, however, have introduced new risks that require unique internal controls. They have engendered the need for new techniques for evaluating controls and for assuring the security and accuracy of corporate data and the information systems that produce it.

This chapter provides an overview of IT auditing. We begin by describing the various types of audits that organizations commission and distinguish between the auditor's traditional attestation responsibility and the emerging field of advisory services. We go on to explain the structure of an IT audit: the relationship between management assertions, audit objectives, tests of controls, and substantive tests are explained. The chapter also outlines the key points of the Committee of Sponsoring Organizations (COSO) control framework, which defines internal controls in both manual and IT environments. The final section of the chapter examines audit issues and implications related to Sarbanes–Oxley legislation and provides a conceptual framework that links general controls, application controls, and financial data integrity. This framework is a model for the remainder of the text.

OVERVIEW OF AUDITING

Business organizations undergo different types of audits for different purposes. The most common of these are external (financial) audits, internal audits, and fraud audits. Each of these is briefly outlined in the following sections.

External (Financial) Audits

An external audit is an independent attestation performed by an expert—the auditor—who expresses an opinion regarding the presentation of financial statements. This task, known as the **attest service**, is performed by Certified Public Accountants (CPAs) who work for public accounting firms that are independent of the client organization being audited. The audit objective is always associated with assuring the fair presentation of financial statements. These audits are, therefore, often referred to as *financial audits*. The Securities and Exchange Commission (SEC) requires all publicly traded companies be subject to a financial audit annually. CPAs conducting such audits represent the interests of outsiders: stockholders, creditors, government agencies, and the general public.

The CPA's role is similar in concept to a judge who collects and evaluates evidence and renders an opinion. A key concept in this process is **independence**. The judge must remain independent in his or her deliberations. The judge cannot be an advocate of either party in the trial, but must apply the law impartially based on the evidence presented. Likewise, the independent auditor collects and evaluates evidence and renders an opinion based on the evidence. Throughout the audit process, the auditor must maintain independence from the client organization. Public confidence in the reliability of the company's internally produced financial statements rests directly on an evaluation of them by an independent auditor.

The external auditor must follow strict rules in conducting financial audits. These authoritative rules have been defined by the SEC, the Financial Accounting Standards Board (FASB), the American Institute of CPA (AICPA), and by federal law (**Sarbanes–Oxley [SOX] Act of 2002**). With the passage of SOX, Congress established the Public Company Accounting Oversight Board (PCAOB), which has to a great extent replaced the function served by the FASB, and some of the functions of the AICPA (e.g., setting standards and issuing reprimands and penalties for CPAs who are convicted of certain crimes or guilty of certain infractions). Regardless, under federal law, the SEC has final authority for financial auditing.

Attest Service versus Advisory Services

An important distinction needs to be made regarding the external auditor's traditional attestation service and the rapidly growing field of advisory services, which many public accounting firms offer. The attest service is defined as:

> an engagement in which a practitioner is engaged to issue, or does issue, a written communication that expresses a conclusion about the reliability of a written assertion that is the responsibility of another party. (SSAE No. 1, AT Sec. 100.01)

The following requirements apply to attestation services:

- Attestation services require written assertions and a practitioner's written report.
- Attestation services require the formal establishment of measurement criteria or their description in the presentation.

- The levels of service in attestation engagements are limited to examination, review, and application of agreed-upon procedures.

Advisory services are professional services offered by public accounting firms to improve their client organizations' operational efficiency and effectiveness. The domain of advisory services is intentionally unbounded so that it does not inhibit the growth of future services that are currently unforeseen. As examples, advisory services include actuarial advice, business advice, fraud investigation services, information system design and implementation, and internal control assessments for compliance with SOX.

Prior to the passage of SOX, accounting firms could provide advisory services concurrently to audit (attest function) clients. SOX legislation, however, greatly restricts the types of nonaudit services that auditors may render to audit clients. It is now unlawful for a registered public accounting firm that is currently providing attest services for a client to provide the following services:

- bookkeeping or other services related to the accounting records or financial statements of the audit client
- financial information systems design and implementation
- appraisal or valuation services, fairness opinions, or contribution-in-kind reports
- actuarial services
- internal audit outsourcing services
- management functions or human resources
- broker or dealer, investment adviser, or investment banking services
- legal services and expert services unrelated to the audit
- any other service that the board determines, by regulation, is impermissible

The advisory services units of public accounting firms responsible for providing IT control-related client support have different names in different firms, but they all engage in tasks known collectively as IT risk management. These groups often play a dual role within their respective firms; they provide nonaudit clients with IT advisory services and also work with their firm's financial audit staff to perform IT-related tests of controls as part of the attestation function.

The material outlined in this chapter relates to tasks that risk management professionals normally conduct during an IT audit. In the pages that follow, we examine what constitutes an audit and how audits are structured. Keep in mind, however, that in many cases the *purpose* of the task, rather than the task itself, defines the service being rendered. For example, a risk management professional may perform a test of IT controls as an advisory service for a nonaudit client who is preparing for a financial audit by a different public accounting firm. The same professional may perform the very same test for an audit client as part of the attest function. Therefore, the issues and procedures described in this text apply to a broader context that includes advisory services and attestation, as well as the internal audit function.

Internal Audits

The Institute of Internal Auditors (IIA) defines **internal auditing** as an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization.[1] Internal auditors perform a wide range of activities on behalf of the organization, including conducting financial audits, examining an operation's

1 AAA Committee on Basic Auditing Concepts, "A Statement of Basic Auditing Concepts," *Accounting Review*, supplement to vol. 47, 1972.

compliance with organizational policies, reviewing the organization's compliance with legal obligations, evaluating operational efficiency, and detecting and pursuing fraud within the firm.

An internal audit is typically conducted by auditors who work for the organization, but this task may be outsourced to other organizations. Internal auditors are often certified as a Certified Internal Auditor (CIA) or a Certified Information Systems Auditor (CISA). While internal auditors self-impose independence to perform their duties effectively, they represent the interests of the organization. These auditors generally answer to executive management of the organization or the audit committee of the board of directors, if one exists. The standards, guidance, and certification of internal audits are governed mostly by the IIA and, to a lesser degree, by the Information Systems Audit and Control Association (ISACA).

External versus Internal Auditors

The characteristic that conceptually distinguishes external auditors from internal auditors is their respective constituencies: while external auditors represent outsiders, internal auditors represent the interests of the organization. Nevertheless, in this capacity, internal auditors often cooperate with and assist external auditors in performing aspects of financial audits. This cooperation is done to achieve audit efficiency and reduce audit fees. For example, a team of internal auditors can perform tests of computer controls under the supervision of a single external auditor.

The independence and competence of the internal audit staff determine the extent to which external auditors may cooperate with and rely on work performed by internal auditors. Internal audit independence implies no subordination of judgment to another and arises from an independent mental attitude that views events on a factual basis without influence from an organizational structure that subordinates the internal audit function. Some internal audit departments report directly to the controller. Under this arrangement, the internal auditor's independence is compromised, and the external auditor is prohibited by professional standards from relying on evidence provided by the internal auditors. In contrast, external auditors can rely in part on evidence gathered by internal audit departments that are organizationally independent and report to the board of directors' audit committee (discussed next). A truly independent internal audit staff adds value to the audit process. For example, internal auditors can gather audit evidence throughout a fiscal period, which external auditors may then use at the year's end to conduct more efficient, less disruptive, and less costly audits of the organization's financial statements.

Fraud Audits

In recent years, fraud audits have, unfortunately, increased in popularity as a corporate governance tool. They have been thrust into prominence by a corporate environment in which both employee theft of assets and major financial frauds by management (e.g., Enron, WorldCom) have become rampant. The objective of a fraud audit is to investigate anomalies and gather evidence of fraud that may lead to criminal conviction. Sometimes fraud audits are initiated by corporate management who suspect employee fraud. Alternatively, boards of directors may hire fraud auditors to look into their own executives if theft of assets or financial fraud is suspected. Organizations victimized by fraud usually contract with specialized fraud units of public accounting firms or with companies that specialize in forensic accounting. Typically, fraud auditors have earned the Certified Fraud Examiner (CFE) certification, which is governed by the Association of Certified Fraud Examiners (ACFE).

THE ROLE OF THE AUDIT COMMITTEE

The board of directors of publicly traded companies form a subcommittee known as the audit committee, which has special responsibilities regarding audits. This committee usually consists of three people who should be outsiders (not associated with the families of executive management nor former officers, etc.). With the advent of the Sarbanes–Oxley Act, at least one member of the audit committee must be a "financial expert." The audit committee serves as an independent "check and balance" for the internal audit function and liaison with external auditors. One of the most significant changes imposed by SOX has been to the relationship between management and the external auditors. Prior to SOX, external auditors were hired and fired by management. Many believe, with some justification, that this relationship erodes auditor independence when disputes over audit practices arise. SOX mandates that external auditors now report to the audit committee who hire and fire auditors and resolve disputes.

To be effective, the audit committee must be willing to challenge the internal auditors (or the entity performing that function) as well as management, when necessary. Part of its role is to look for ways to identify risk. For instance, it might serve as a sounding board for employees who observe suspicious behavior or spot fraudulent activities. In general, it becomes an independent guardian of the entity's assets by whatever means is appropriate. Corporate frauds often have some bearing on audit committee failures. These include lack of independence of audit committee members, inactive audit committees, total absence of an audit committee, and lack of experienced members on the audit committee.

FINANCIAL AUDIT COMPONENTS

The product of the attestation function is a formal written report that expresses an opinion about the reliability of the assertions contained in the financial statements. The auditor's report expresses an opinion as to whether the financial statements are in conformity with *generally accepted accounting principles (GAAP)*; external users of financial statements are presumed to rely on the auditor's opinion about the reliability of financial statements in making decisions. To do so, users must be able to place their trust in the auditor's competence, professionalism, integrity, and independence. Auditors are guided in their professional responsibility by the 10 *generally accepted auditing standards (GAAS)* presented in Table 1.1.

Auditing Standards

Auditing standards are divided into three classes: general qualification standards, field work standards, and reporting standards. GAAS establishes a framework for prescribing auditor performance, but it is not sufficiently detailed to provide meaningful guidance in specific circumstances. To provide specific guidance, the AICPA issues *Statements on Auditing Standards (SASs)* as authoritative interpretations of GAAS. SASs are often referred to as *auditing standards*, or *GAAS*, although they are not the 10 generally accepted auditing standards.

The first SAS (SAS 1) was issued by the AICPA in 1972. Since then, many SASs have been issued to provide auditors with guidance on a spectrum of topics, including methods of investigating new clients, procedures for collecting information from

TABLE 1.1 Generally Accepted Auditing Standards

General Standards	Standards of Field Work	Reporting Standards
1. The auditor must have adequate technical training and proficiency.	1. Audit work must be adequately planned.	1. The auditor must state in the report whether financial statements were prepared in accordance with generally accepted accounting principles.
2. The auditor must have independence of mental attitude.	2. The auditor must gain a sufficient understanding of the internal control structure.	2. The report must identify those circumstances in which generally accepted accounting principles were not applied.
3. The auditor must exercise due professional care in the performance of the audit and the preparation of the report.	3. The auditor must obtain sufficient, competent evidence.	3. The report must identify any items that do not have adequate informative disclosures.
		4. The report shall contain an expression of the auditor's opinion on the financial statements as a whole.

attorneys regarding contingent liability claims against clients, and techniques for obtaining background information on the client's industry.

Statements on Auditing Standards are regarded as authoritative pronouncements because every member of the profession must follow their recommendations or be able to show why a SAS does not apply in a given situation. The burden of justifying departures from the SASs falls upon the individual auditor.

A Systematic Process

Conducting an audit is a systematic and logical process that applies to all forms of information systems. While important in all audit settings, a systematic approach is particularly important in the IT environment. The lack of physical procedures that can be visually verified and evaluated injects a high degree of complexity into the IT audit (e.g., the audit trail may be purely electronic, in a digital form, and thus invisible to those attempting to verify it). Therefore, a logical framework for conducting an audit in the IT environment is critical to help the auditor identify all-important processes and data files.

Management Assertions and Audit Objectives

The organization's financial statements reflect a set of **management assertions** about the financial health of the entity. The task of the auditor is to determine whether the financial statements are fairly presented. To accomplish this goal, the auditor establishes **audit objectives**, designs procedures, and gathers evidence that corroborate or refute management's assertions. These assertions fall into five general categories:

1. The **existence or occurrence** assertion affirms that all assets and equities contained in the balance sheet exist and that all transactions in the income statement actually occurred.
2. The **completeness** assertion declares that no material assets, equities, or transactions have been omitted from the financial statements.

3. The **rights and obligations** assertion maintains that assets appearing on the balance sheet are owned by the entity and that the liabilities reported are obligations.
4. The **valuation or allocation** assertion states that assets and equities are valued in accordance with GAAP and that allocated amounts such as depreciation expense are calculated on a systematic and rational basis.
5. The **presentation and disclosure** assertion alleges that financial statement items are correctly classified (e.g., long-term liabilities will not mature within one year) and that footnote disclosures are adequate to avoid misleading the users of financial statements.

Generally, auditors develop their audit objectives and design **audit procedures** based on the preceding assertions. The example in Table 1.2 outlines these procedures.

Audit objectives may be classified into two general categories. Those in Table 1.2 relate to transactions and account balances that directly impact financial reporting. The second category pertains to the information system itself. This category includes the audit objectives for assessing controls over manual operations and computer technologies used in transaction processing. In the chapters that follow, we consider both categories of audit objectives and the associated audit procedures.

Obtaining Evidence

Auditors seek evidential matter that corroborates management assertions. In the IT environment, this process involves gathering evidence relating to the reliability of computer controls as well as the contents of databases that have been processed by computer programs. Evidence is collected by performing tests of controls, which establish whether internal controls are functioning properly, and substantive tests, which determine whether accounting databases fairly reflect the organization's transactions and account balances.

Ascertaining Materiality

The auditor must determine whether weaknesses in internal controls and misstatements found in transactions and account balances are material. In all audit environments,

TABLE 1.2 **Audit Objectives and Audit Procedures Based on Management Assertions**

Management Assertion	Audit Objective	Audit Procedure
Existence or occurrence	Inventories listed on the balance sheet exist.	Observe the counting of physical inventory.
Completeness	Accounts payable include all obligations to vendors for the period.	Compare receiving reports, supplier invoices, purchase orders, and journal entries for the period and the beginning of the next period.
Rights and obligations	Plant and equipment listed in the balance sheet are owned by the entity.	Review purchase agreements, insurance policies, and related documents.
Valuation or allocation	Accounts receivable are stated at net realizable value.	Review entity's aging of accounts and evaluate the adequacy of the allowance for uncorrectable accounts.
Presentation and disclosure	Contingencies not reported in financial accounts are properly disclosed in footnotes.	Obtain information from entity lawyers about the status of litigation and estimates of potential loss.

assessing materiality is an auditor judgment. In an IT environment, however, this decision is complicated further by technology and a sophisticated internal control structure.

Communicating Results

Auditors must communicate the results of their tests to interested users. An independent auditor renders a report to the audit committee of the board of directors or stockholders of a company. The audit report contains, among other things, an **audit opinion**. This opinion is distributed along with the financial report to interested parties both internal and external to the organization. IT auditors often communicate their findings to internal and external auditors, who can then integrate these findings with the non-IT aspects of the audit.

AUDIT RISK

Audit risk is the probability that the auditor will render an unqualified (clean) opinion on financial statements that are, in fact, materially misstated. Material misstatements may be caused by errors or irregularities or both. Errors are unintentional mistakes. Irregularities are intentional misrepresentations associated with the commission of a fraud such as the misappropriation of physical assets or the deception of financial statement users.

Audit Risk Components

The auditor's objective is to achieve a level of audit risk that is acceptable to the auditor. Acceptable audit risk (AR) is estimated based on the *ex ante* value of the components of the audit risk model. These are inherent risk, control risk, and detection risk.

Inherent Risk

Inherent risk is associated with the unique characteristics of the business or industry of the client.[2] Firms in declining industries have greater inherent risk than firms in stable or thriving industries. Likewise, industries that have a heavy volume of cash transactions have a higher level of inherent risk than those that do not. Furthermore, placing a value on inventory when the inventory value is difficult to assess due to its nature is associated with higher inherent risk than in situations where inventory values are more objective. For example, the valuation of diamonds is inherently more risky than assessing the value of automobile tires. Auditors cannot reduce the level of inherent risk. Even in a system protected by excellent controls, financial data and, consequently, financial statements, can be materially misstated.

Control risk is the likelihood that the control structure is flawed because controls are either absent or inadequate to prevent or detect errors in the accounts.[3] To illustrate

2 Institute of Internal Auditors, *Standards of Professional Practice of Internal Auditing* (Orlando, FL: Institute of Internal Auditors, 1978).

3 Auditing Standards Board, *AICPA Professional Standards* (New York: AICPA, 1994), AU Sec. 312.20.

control risk, consider the following partial customer sales record, which is processed by the sales order system.

Quantity	Unit Price	Total
10 Units	$20	$2,000

Assuming the Quantity and Unit Price fields in the record are correctly presented, the extended amount (Total) value of $2,000 is in error. An accounting information system (AIS) with adequate controls should prevent or detect such an error. If, however, controls are lacking and the value of Total in each record is not validated before processing, then the risk of undetected errors entering the data files increases.

Auditors assess the level of control risk by performing tests of internal controls. In the preceding example, the auditor could create test transactions, including some with incorrect Total values, which are processed by the application in a test run. The results of the test will indicate that price extension errors are not detected and are being incorrectly posted to the accounts receivable file.

Detection Risk

Detection risk is the risk that auditors are willing to take that errors not detected or prevented by the control structure will also not be detected by the auditor. Auditors set an acceptable level of detection risk (planned detection risk) that influences the level of substantive tests that they perform. For example, more substantive testing would be required when the planned detection risk is 10 percent than when it is 20 percent.

Audit Risk Model

Financial auditors use the audit risk components in a model to determine the scope, nature, and timing of substantive tests. The audit risk model is

$$AR = IR \times CR \times DR$$

Assume that acceptable audit risk is assessed at a value of 5 percent, consistent with the 95 percent confidence interval associated with statistics. By illustration, assume IR is assessed at 40 percent, and CR is assessed at 60 percent. What would be the level of planned detection risk (DR) needed to achieve the acceptable audit risk (AR) of 5 percent?

$$5\% = 40\% \times 60\% \times DR$$
$$DR = .05/.24$$
$$DR = .20$$

Let's now reduce the control risk (CR) value to 40 percent and recalculate DR.

$$5\% = 40\% \times 40\% \times DR$$
$$DR = .31$$

Notice that to achieve an acceptable level of audit risk in the first example, the auditor must set planned detection risk lower (20 percent) than in the second example (31 percent). This is because the internal control structure in the first example is more risky (60 percent) than it is in the second case (40 percent). To achieve the planned detection of 20 percent in the first example, the auditor will need to perform more substantive tests than in the second example, where the risk is lower. This relationship is explained next.

The Relationship Between Tests of Controls and Substantive Tests

Tests of controls and substantive tests are auditing techniques used for reducing audit risk to an acceptable level. The stronger the internal control structure, as determined through tests of controls, the lower the control risk and the less substantive testing the auditor must do. This relationship is true because the likelihood of errors in the accounting records is reduced when controls are strong. In other words, when controls are in place and effective, the auditor may limit substantive testing. In contrast, the weaker the internal control structure, the greater the control risk and the more substantive testing the auditor must perform to reduce total audit risk. Evidence of weak controls forces the auditor to extend substantive testing to search for misstatements.

In summary, the more reliable the internal controls, the lower the CR probability. That leads to a lower DR, which will lead to fewer substantive tests being required. Because substantive tests are labor intensive and time-consuming, they drive up audit costs and exacerbate the disruptive effects of an audit. Thus, management's best interests are served by having a strong internal control structure.

THE IT AUDIT

The public expression of the auditor's opinion is the culmination of a systematic financial audit process that involves three conceptual phases: audit planning, tests of controls, and substantive testing. Figure 1.1 illustrates the steps involved in these phases. An IT audit focuses on the computer-based aspects of an organization's information system; and modern systems employ significant levels of technology. For example, transaction processing is automated and performed in large part by computer programs. Similarly source documents, journals, and ledgers that traditionally were paper-based are now digitized and stored in relational databases. As we will see later, the controls over these processes and databases become central issues in the financial audit process.

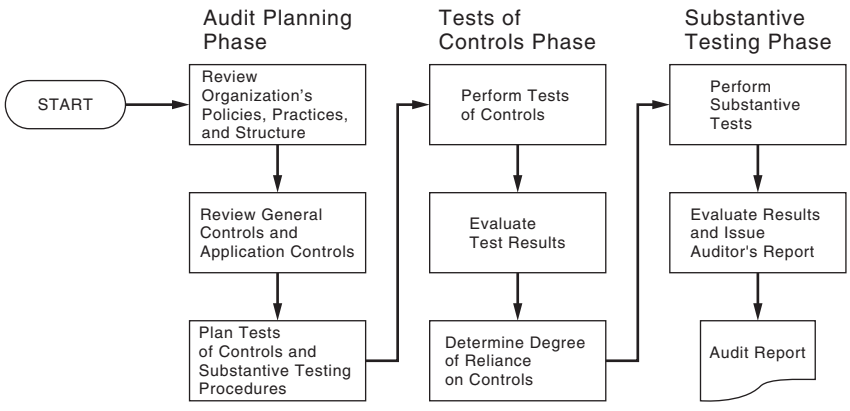
The Structure of an IT Audit

Audit Planning

The first step in the IT audit is **audit planning**. Before the auditor can determine the nature and extent of the tests to perform, he or she must gain a thorough understanding

FIGURE 1.1

Phases of an IT Audit



of the client's business. A major part of this phase of the audit is the analysis of audit risk. The auditor's objective is to obtain sufficient information about the firm to plan the other phases of the audit. The risk analysis incorporates an overview of the organization's internal controls. During the review of controls, the auditor attempts to understand the organization's policies, practices, and structure. In this phase of the audit, the auditor also identifies the financially significant applications and attempts to understand the controls over the primary transactions that are processed by these applications.

The techniques for gathering evidence at this phase include conducting questionnaires, interviewing management, reviewing systems documentation, and observing activities. During this process, the IT auditor must identify the principal exposures and the controls that attempt to reduce these exposures. Having done so, the auditor proceeds to the next phase, where he or she tests the controls for compliance with preestablished standards.

Tests of Controls

The objective of the **tests of controls** phase is to determine whether adequate internal controls are in place and functioning properly. To accomplish this, the auditor performs various tests of controls. The evidence-gathering techniques used in this phase may include both manual techniques and specialized computer audit techniques. We shall examine several such methods later in this text.

At the conclusion of the tests of controls phase, the auditor must assess the quality of the internal controls by assigning a level for control risk. As previously explained, the degree of reliance that the auditor can ascribe to internal controls will affect the nature and extent of substantive testing that needs to be performed.

Substantive Testing

The third phase of the audit process focuses on financial data. This phase involves a detailed investigation of specific account balances and transactions through what are called **substantive tests**. For example, a customer confirmation is a substantive test sometimes used to verify account balances. The auditor selects a sample of accounts receivable balances and traces these back to their source—the customers—to determine if the amount stated is in fact owed by a bona fide customer. By so doing, the auditor can verify the accuracy of each account in the sample. Based on such sample findings, the auditor is able to draw conclusions about the fair value of the entire accounts receivable asset.

Some substantive tests are physical, labor-intensive activities, such as counting cash, counting inventories in the warehouse, and verifying the existence of stock certificates in a safe. In an IT environment, the data needed to perform substantive tests (such as account balances and names and addresses of individual customers) are contained in data files that often must be extracted using **Computer-Assisted Audit Tools and Techniques (CAATTs)** software. In a later chapter of this text, we will examine the role of CAATTs in performing traditional substantive tests and other data analysis and reporting tasks.

INTERNAL CONTROL

Organization management is required by law to establish and maintain an adequate system of internal control. Consider the following Securities and Exchange Commission statement on this matter:

> The establishment and maintenance of a system of internal control is an important management obligation. A fundamental aspect of management's stewardship responsibility

> is to provide shareholders with reasonable assurance that the business is adequately controlled. Additionally, management has a responsibility to furnish shareholders and potential investors with reliable financial information on a timely basis.[4]

Brief History of Internal Control Legislation

Since much of the internal control system relates directly to transaction processing, accountants are key participants in ensuring control adequacy. This section begins with a brief history of internal controls, and then provides a conceptual overview of internal control. Lastly, it presents the COSO control framework.

SEC Acts of 1933 and 1934

Following the stock market crash of 1929, and a worldwide financial fraud by Ivar Kreugar, the U.S. legislature passed two acts to restore confidence in the capital market. The first was the Securities Act of 1933, which had two main objectives: (1) require that investors receive financial and other significant information concerning securities being offered for public sale; and (2) prohibit deceit, misrepresentations, and other fraud in the sale of securities. The second act, the Securities Exchange Act, 1934, created the Securities and Exchange Commission (SEC) and empowered it with broad authority over all aspects of the securities industry, which included authority regarding auditing standards. The SEC acts also required publicly traded companies to be audited by an independent auditor (i.e., CPA). But is also required all companies that report to the SEC to maintain a system of internal control that is evaluated as part of the annual external audit. That portion of the Act has been enforced on rare occasions. That leniency changed with the passage of Sarbanes–Oxley Act in July 2002, discussed later.

Copyright Law—1976

This law, which has had multiple revisions, added software and other intellectual properties into the existing copyright protection laws. It is of concern to IT auditors because management is held personally liable for violations (e.g., software piracy) if "raided" by the software police (a U.S. marshal accompanied by software vendors' association representatives), and sufficient evidence of impropriety is found.

Foreign Corrupt Practices Act (FCPA) of 1977

Corporate management has not always lived up to its internal control responsibility. With the discovery that U.S. business executives were using their organizations' funds to bribe foreign officials, internal control issues, formerly of little interest to stockholders, quickly became a matter of public concern. From this issue came the passage of the **Foreign Corrupt Practices Act of 1977 (FCPA)**. Among its provisions, the FCPA requires companies registered with the SEC to do the following:

1. Keep records that fairly and reasonably reflect the transactions of the firm and its financial position.
2. Maintain a system of internal control that provides reasonable assurance that the organization's objectives are met.

The FCPA has had a significant impact on organization management. With the knowledge that violation of the FCPA could lead to heavy fines and imprisonment, managers have developed a deeper concern for control adequacy.

4 Ibid.

Committee of Sponsoring Organizations—1992

Following the series of S&L scandals of the 1980s, a committee was formed to address these frauds. Originally, the committee took the name of its chair, Treadway, but eventually the project became known as **COSO**. The sponsoring organizations included Financial Executives International (FEI), the Institute of Management Accountants (IMA), the American Accounting Association (AAA), AICPA, and the IIA. The Committee spent several years promulgating a response. Because it was determined early on that the best deterrent to fraud was strong internal controls, the committee decided to focus on an effective model for internal controls from a management perspective. The result was the COSO Model. The AICPA adopted the model into auditing standards and published SAS No. 78—*Consideration of Internal Control in a Financial Statement Audit*.

Sarbanes–Oxley Act of 2002

As a result of several large financial frauds (e.g., Enron, Worldcom, Adelphia) and the resulting losses suffered by stockholders, pressure was brought by the U.S. Congress to protect the public from such events. This led to the passage of the Sarbanes–Oxley Act (SOX) on July 30, 2002. In general, the law supports efforts to increase public confidence in capital markets by seeking to improve corporate governance, internal controls, and audit quality.

In particular, SOX requires management of public companies to implement an adequate system of internal controls over their financial reporting process. This includes controls over transaction processing systems that feed data to the financial reporting systems. Management's responsibilities for this are codified in Sections 302 and 404 of SOX.

Section 302 requires that corporate management (including the CEO) certify their organization's internal controls on a quarterly and annual basis. Section 302 also carries significant auditor implications. Specifically, external auditors must perform the following procedures quarterly to identify any material modifications in controls that may impact financial reporting:

- Interview management regarding any significant changes in the design or operation of internal control that occurred subsequent to the preceding annual audit or prior review of interim financial information.
- Evaluate the implications of misstatements identified by the auditor as part of the interim review that relate to effective internal controls.
- Determine whether changes in internal controls are likely to materially affect internal control over financial reporting.

In addition, Section 404 requires the management of public companies to assess the effectiveness of their organization's internal controls. This entails providing an annual report addressing the following points:

1. Understand the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise.
2. Using a risk-based approach, assess both the design and operating effectiveness of selected internal controls related to material accounts.[5]
3. Assess the potential for fraud in the system and evaluate the controls designed to prevent or detect fraud.
4. Evaluate and conclude on the adequacy of controls over the financial statement reporting process.

5 Securities and Exchange Commission, Securities Release 34-13185 (January 19, 1977).

5. Evaluate entity-wide (general) controls that correspond to the components of the COSO framework.

Regarding the control framework, the SEC has made specific reference to COSO as a recommended model. Furthermore, the PCAOB Auditing Standard No. 5 endorses the use of COSO as the framework for control assessment. Although other suitable frameworks have been published, any framework used should encompass all of COSO's general themes.[6] The key elements of the COSO framework are presented in a later section.

INTERNAL CONTROL OBJECTIVES, PRINCIPLES, AND MODELS

An organization's **internal control system** comprises policies, practices, and procedures to achieve four broad objectives:

1. To safeguard assets of the firm.
2. To ensure the accuracy and reliability of accounting records and information.
3. To promote efficiency in the firm's operations.
4. To measure compliance with management's prescribed policies and procedures.[7]

Modifying Principles

Inherent in these control objectives are four modifying principles that guide designers and auditors of internal control systems.[8]

Management Responsibility

This concept holds that the establishment and maintenance of a system of internal control is a management responsibility. Although the FCPA supports this principle, SOX legislation makes it law!

Methods of Data Processing

The internal control system should achieve the four broad objectives regardless of the **data processing** method used (whether manual or computer based). However, the specific techniques used to achieve these objectives will vary with different types of technology.

Limitations

Every system of internal control has **limitations** on its effectiveness. These include (1) the possibility of error—no system is perfect, (2) circumvention—personnel may circumvent the system through collusion or other means, (3) management override—management is in a position to override control procedures by personally distorting transactions or by directing a subordinate to do so, and (4) changing conditions—conditions may change over time so that existing effective controls may become ineffectual.

---

6 A popular competing control framework is Control Objectives for Information and related Technology (COBIT®) published by the IT Governance Institute (ITGI). This framework maps into COSO's general themes.

7 American Institute of Certified Public Accountants, *AICPA Professional Standards*, vol. 1 (New York: AICPA, 1987) AU Sec. 320. 30–35.

8 American Institute of Certified Public Accountants, Committee on Auditing Procedure, Internal Control—Elements of a Coordinated System and Its Importance to Management and the Independent Public Accountant, *Statement on Auditing Standards No. 1*, Sec. 320 (New York: AICPA, 1973).

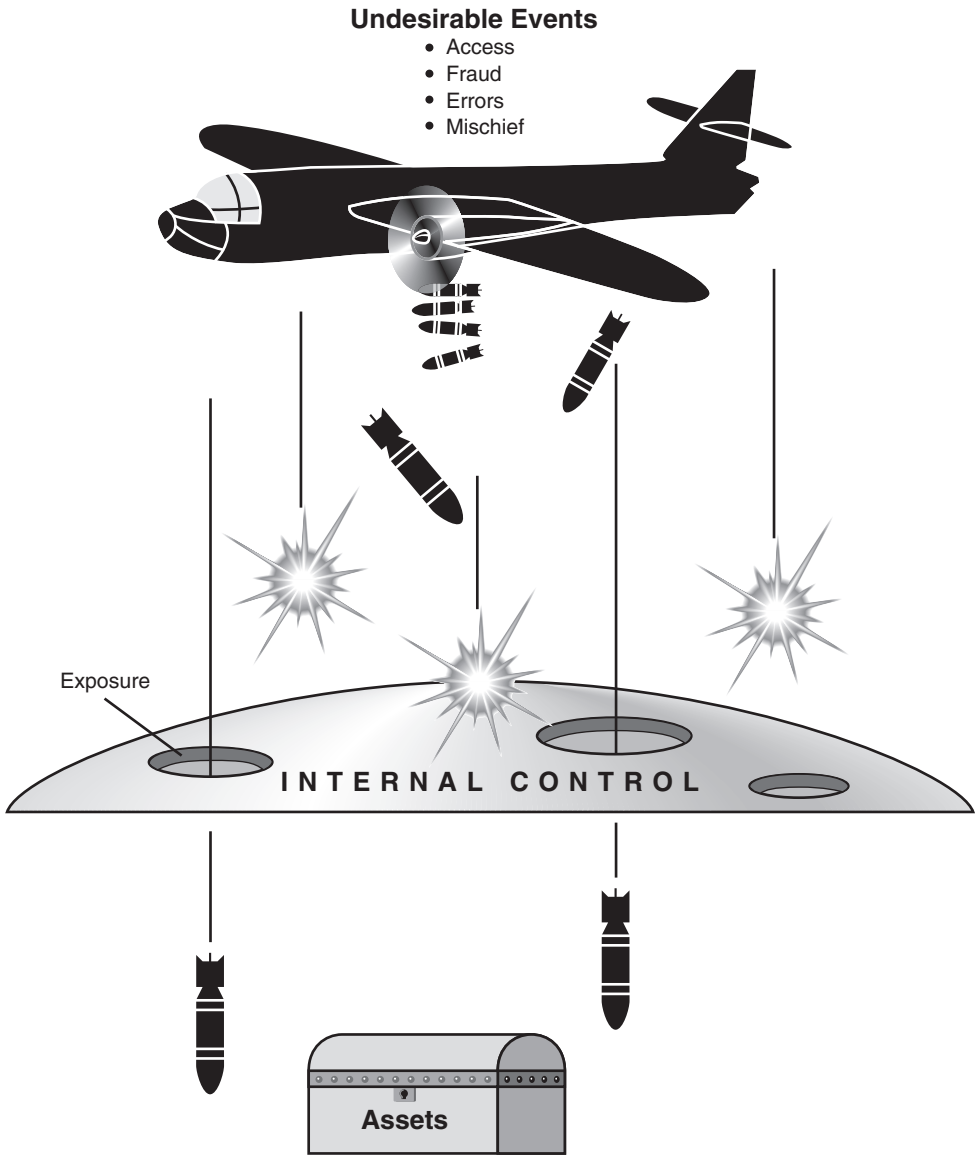
Reasonable Assurance

The internal control system should provide **reasonable assurance** that the four broad objectives of internal control are met. This reasonableness means that the cost of achieving improved control should not outweigh its benefits.

To illustrate the limitations and reasonable-assurance principles, Figure 1.2 portrays the internal control system as a shield that protects the firm's assets from numerous undesirable events that bombard the organization. These include attempts at unauthorized access to the firm's assets (including information); fraud perpetrated by persons both in and outside the firm; errors due to employee incompetence, faulty computer programs, and corrupted input data; and mischievous acts, such as unauthorized access by computer hackers and threats from computer viruses that destroy programs and databases.

FIGURE 1.2

Internal Control Shield



Absence of or weakness in controls are illustrated in Figure 1.2 as holes in the control shield. Some weaknesses are immaterial and tolerable. Under the principle of reasonable assurance, these control weaknesses may not be worth fixing. Material weaknesses in controls, however, increase the firm's risk to financial loss or injury from the undesirable events. The cost of correcting these weaknesses is offset by the benefits derived.

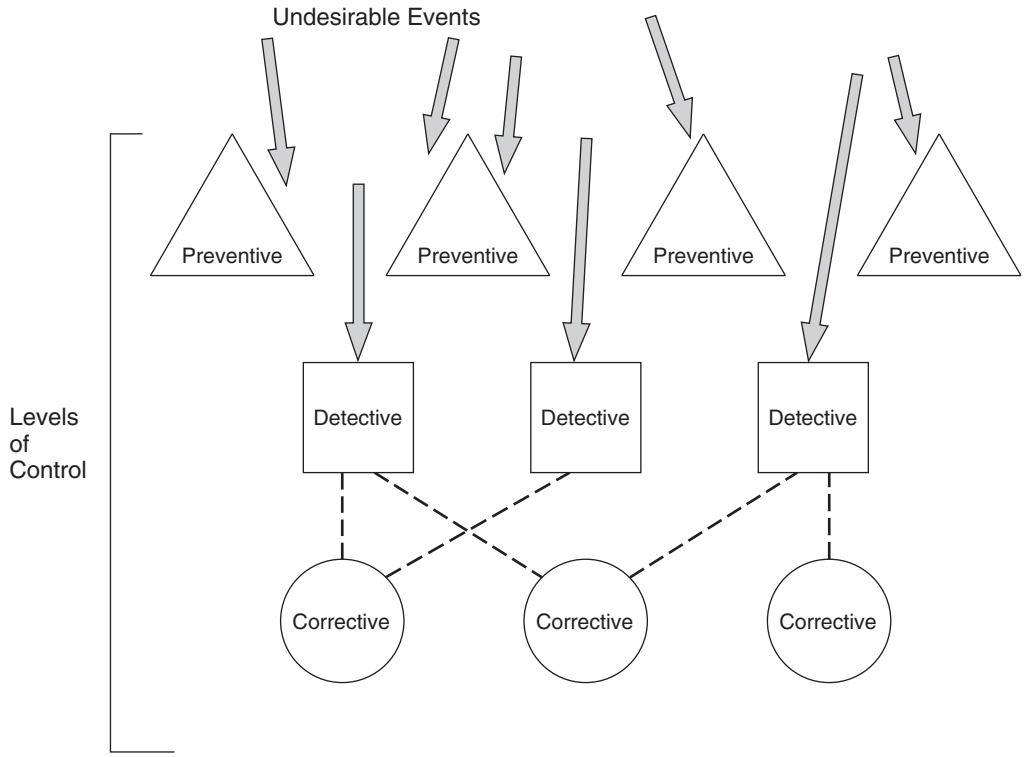
The PDC Model

Figure 1.3 illustrates that the internal control shield represented in Figure 1.2 actually consists of three levels of control: preventive controls, detective controls, and corrective controls. This is called the **PDC control model**.

Preventive Controls

Prevention is the first line of defense in the control structure. **Preventive controls** are passive techniques designed to reduce the frequency of occurrence of undesirable events. Preventive controls force compliance with prescribed or desired actions and thus screen out aberrant events. When designing internal control systems, an ounce of prevention is most certainly worth a pound of cure. Preventing errors and fraud is far more cost-effective than detecting and correcting problems after they occur. The vast majority of undesirable events can be blocked at this first level. For example, a well-designed data entry screen is an example of a preventive control. The logical layout of the screen into zones that permit only specific types of data, such as customer name, address, items sold, and quantity, forces the data entry clerk to enter the required data and prevents necessary data from being omitted.

FIGURE 1.3 **Preventive, Detective, and Corrective Controls**



Detective Controls

Detection of problems is the second line of defense. **Detective controls** are devices, techniques, and procedures designed to identify and expose undesirable events that elude preventive controls. Detective controls reveal specific types of errors by comparing actual occurrences to preestablished standards. When the detective control identifies a departure from standard, it sounds an alarm to attract attention to the problem. For example, assume that because of a data entry error, a customer sales order record contains the following data:

Quantity	Unit Price	Total
10	$10	$1,000

Before processing this transaction and posting to the accounts, a detective control should recalculate the total value using the price and quantity. Thus, this error above would be detected.

Corrective Controls

Corrective actions must be taken to reverse the effects of detected errors. There is an important distinction between detective controls and corrective controls. Detective controls identify undesirable events and draw attention to the problem; **corrective controls** actually fix the problem. For any detected error, there may be more than one feasible corrective action, but the best course of action may not always be obvious. For example, in viewing the preceding error, your first inclination may have been to change the total value from $1,000 to $100 to correct the problem. This presumes that the quantity and price values in the record are correct; they may not be. At this point, we cannot determine the real cause of the problem; we know only that one exists.

Linking a corrective action to a detected error, as an automatic response, may result in an incorrect action that causes a worse problem than the original error. For this reason, error correction should be viewed as a separate control step that should be taken cautiously.

The PDC control model is conceptually pleasing but offers little practical guidance for designing or auditing specific controls. The current authoritative document for specifying internal control objectives and techniques is the **Statement on Auditing Standards No. 109 (SAS 109)**, which is based on the COSO framework. SAS 109 describes the complex relationship between the firm's internal controls, the auditor's assessment of risk, and the planning of audit procedures. SAS 109 provides guidance to auditors in their application of the COSO framework when assessing the risk of material misstatement. We now discuss the key elements of this framework.

COSO Internal Control Framework

The COSO framework consists of five components: the control environment, risk assessment, information and communication, monitoring, and control activities.

The Control Environment

The **control environment** is the foundation for the other four control components. The control environment sets the tone for the organization and influences the control awareness of its management and employees. Important elements of the control environment are:

- The integrity and ethical values of management.
- The structure of the organization.

- The participation of the organization's board of directors and the audit committee, if one exists.
- Management's philosophy and operating style.
- The procedures for delegating responsibility and authority.
- Management's methods for assessing performance.
- External influences, such as examinations by regulatory agencies.
- The organization's policies and practices for managing its human resources.

SAS 109 requires that auditors obtain sufficient knowledge to assess the attitude and awareness of the organization's management, board of directors, and owners regarding internal control. The following paragraphs provide examples of techniques that may be used to obtain an understanding of the control environment.

1. Auditors should assess the integrity of the organization's management and may use investigative agencies to report on the backgrounds of key managers. Some of the "Big Four" public accounting firms employ former FBI agents whose primary responsibility is to perform background checks on existing and prospective clients. If cause for serious reservations comes to light about the integrity of the client, the auditor should withdraw from the audit. The reputation and integrity of the company's managers are critical factors in determining the auditability of the organization. Auditors cannot function properly in an environment in which client management is deemed unethical and corrupt.
2. Auditors should be aware of conditions that would predispose the management of an organization to commit fraud. Some of the obvious conditions may be lack of sufficient working capital, adverse industry conditions, bad credit ratings, and the existence of extremely restrictive conditions in bank or indenture agreements. If auditors encounter any such conditions, their examination should give due consideration to the possibility of fraudulent financial reporting. Appropriate measures should be taken, and every attempt should be made to uncover any fraud.
3. Auditors should understand a client's business and industry and should be aware of conditions peculiar to the industry that may affect the audit. Auditors should read industry-related literature and familiarize themselves with the risks that are inherent in the business.
4. The board of directors should adopt, as a minimum, the provisions of SOX. In addition, the following guidelines represent established best practices.
    - *Separate CEO and chairman.* The roles of CEO and board chairman should be separate. Executive sessions give directors the opportunity to discuss issues without management present, and an independent chairman is important in facilitating such discussions.
    - *Set ethical standards.* The board of directors should establish a code of ethical standards from which management and staff will take direction. At a minimum, a code of ethics should address such issues as outside employment conflicts, acceptance of gifts that could be construed as bribery, falsification of financial and/or performance data, conflicts of interest, political contributions, confidentiality of company and customer data, honesty in dealing with internal and external auditors, and membership on external boards of directors.
    - *Establish an independent audit committee.* The audit committee is responsible for selecting and engaging an independent auditor, ensuring that an annual audit is conducted, reviewing the audit report, and ensuring that deficiencies are addressed. Large organizations with complex accounting practices may need to create audit subcommittees that specialize in specific activities.

- *Compensation committees.* The compensation committee should not be a rubber stamp for management. Excessive use of short-term stock options to compensate directors and executives may result in decisions that influence stock prices at the expense of the firm's long-term health. Compensation schemes should be carefully evaluated to ensure that they create the desired incentives.
- *Nominating committees.* The board nominations committee should have a plan to maintain a fully staffed board of directors with capable people as it moves forward for the next several years. The committee must recognize the need for independent directors and have criteria for determining independence. For example, under its newly implemented governance standards, General Electric (GE) considers directors independent if the sales to, and purchases from, GE total less than 1 percent of the revenue of the companies for which they serve as executives. Similar standards apply to charitable contributions from GE to any organization on which a GE director serves as officer or director. In addition, the company has set a goal that two-thirds of the board will be independent nonemployees.[9]
- *Access to outside professionals.* All committees of the board should have access to attorneys and consultants other than the corporation's normal counsel and consultants. Under the provisions of SOX, the audit committee of an SEC reporting company is entitled to such representation independently.

Risk Assessment

Organizations must perform a **risk assessment** to identify, analyze, and manage risks relevant to financial reporting. Risks can arise or change from circumstances such as:

- Changes in the operating environment that impose new or changed competitive pressures on the firm.
- New personnel who have a different or inadequate understanding of internal control.
- New or reengineered information systems that affect transaction processing.
- Significant and rapid growth that strains existing internal controls.
- The implementation of new technology into the production process or information system that impacts transaction processing.
- The introduction of new product lines or activities with which the organization has little experience.
- Organizational restructuring resulting in the reduction and/or reallocation of personnel such that business operations and transaction processing are affected.
- Entering into foreign markets that may impact operations (i.e., the risks associated with foreign currency transactions).
- Adoption of a new accounting principle that impacts the preparation of financial statements.

SAS 109 requires that auditors obtain sufficient knowledge of the organization's risk assessment procedures to understand how management identifies, prioritizes, and manages the risks related to financial reporting.

Information and Communication

The accounting information system consists of the records and methods used to initiate, identify, analyze, classify, and record the organization's transactions and to account for

9 Rachel E. Silverman, "GE Makes Changes in Board Policy," *The Wall Street Journal* (New York: November 8, 2002).

the related assets and liabilities. The quality of information that the accounting information system generates impacts management's ability to take actions and make decisions in connection with the organization's operations and to prepare reliable financial statements. An effective accounting information system will:

- Identify and record all valid financial transactions.
- Provide timely information about transactions in sufficient detail to permit proper classification and financial reporting.
- Accurately measure the financial value of transactions so their effects can be recorded in financial statements.
- Accurately record transactions in the time period in which they occurred.

SAS 109 requires that auditors obtain sufficient knowledge of the organization's information system to understand:

- The classes of transactions that are material to the financial statements and how those transactions are initiated.
- The accounting records and accounts that are used in the processing of material transactions.
- The transaction processing steps involved from the initiation of a transaction to its inclusion in the financial statements.
- The financial reporting process used to prepare financial statements, disclosures, and accounting estimates.

Monitoring

Management must determine that internal controls are functioning as intended. **Monitoring** is the process by which the quality of internal control design and operation can be assessed. This may be accomplished by separate procedures or by ongoing activities.

An organization's internal auditors may monitor the entity's activities in separate procedures. They gather evidence of control adequacy by testing controls and then communicate control strengths and weaknesses to management. As part of this process, internal auditors make specific recommendations for improvements to controls.

Ongoing monitoring may be achieved by integrating special computer modules into the information system that capture key data and/or permit tests of controls to be conducted as part of routine operations. Embedded modules thus allow management and auditors to maintain constant surveillance over the functioning of internal controls. In Chapter 7, we examine a number of embedded module techniques and related audit tools.

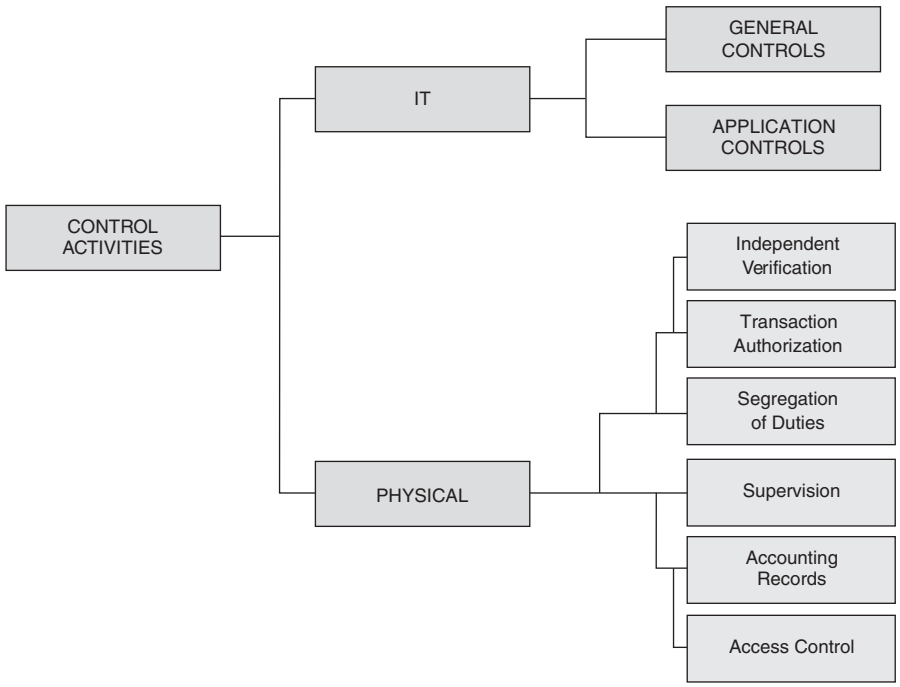
Another technique for achieving ongoing monitoring is the judicious use of management reports. Timely reports allow managers in functional areas such as sales, purchasing, production, and cash disbursements to oversee and control their operations. By summarizing activities, highlighting trends, and identifying exceptions from normal performance, well-designed management reports provide evidence of internal control function or malfunction.

Control Activities

Control activities are the policies and procedures used to ensure that appropriate actions are taken to deal with the organization's identified risks. Control activities can be grouped into two distinct categories: *physical controls* and *information technology (IT) controls*. Figure 1.4 illustrates control activities in their respective categories.

FIGURE 1.4

Categories of Control Activities



Physical Controls

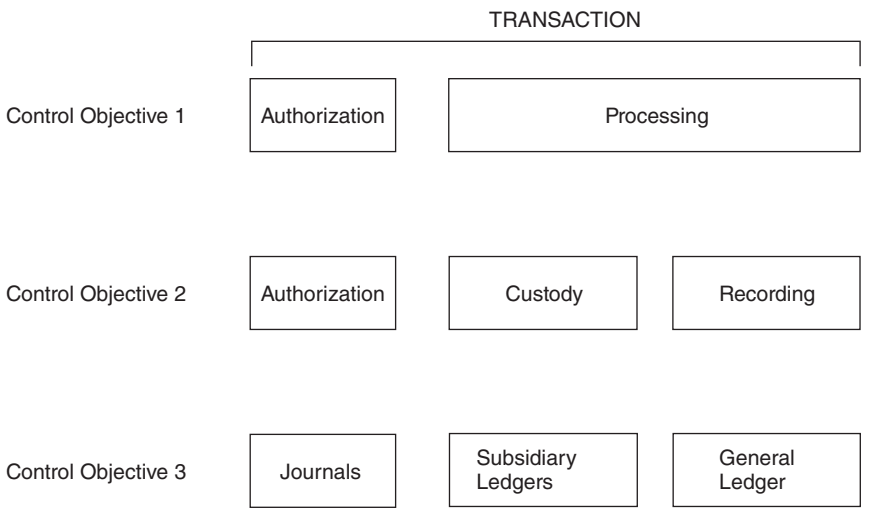
This class of controls relates primarily to the human activities employed in accounting systems. These activities may be purely manual, such as the physical custody of assets, or they may involve the *physical* use of computers to record transactions or update accounts. Physical controls do not relate to the computer logic that actually performs accounting tasks. Rather, they relate to the human activities that trigger and utilize the results of those tasks. In other words, physical controls focus on people, but are not restricted to an environment in which clerks update paper accounts with pen and ink. Virtually all systems, regardless of their sophistication, employ human activities that need to be controlled.

Our discussion will address the issues pertaining to six categories of physical control activities: transaction authorization, segregation of duties, supervision, accounting records, access control, and independent verification.

Transaction Authorization. The purpose of **transaction authorization** is to ensure that all material transactions processed by the information system are valid and in accordance with management's objectives. Authorizations may be general or specific. General authority is granted to operations personnel to perform day-to-day activities. An example of general authorization is the procedure to authorize the purchase of inventories from a designated vendor only when inventory levels fall to their predetermined reorder points. This is called a programmed procedure (not necessarily in the computer sense of the word) in which the decision rules are specified in advance, and no additional approvals are required. On the other hand, specific authorizations deal with case-by-case decisions associated with nonroutine transactions. An example of this is the decision to extend a particular customer's credit limit beyond the normal amount. Specific authority is usually a management responsibility.

FIGURE 1.5

Segregation of Duties Objectives



Segregation of Duties. One of the most important control activities is the segregation of employee duties to minimize incompatible functions. **Segregation of duties** can take many forms, depending on the specific duties to be controlled. However, the following three objectives provide general guidelines applicable to most organizations. These objectives are illustrated in Figure 1.5.

Objective 1. The segregation of duties should be such that the authorization for a transaction is separate from the processing of the transaction. For example, the purchasing department should not initiate purchases until the inventory control department gives authorization. This separation of tasks is a control to prevent individuals from purchasing unnecessary inventory.

Objective 2. Responsibility for asset custody should be separate from the record-keeping responsibility. For example, the department that has physical custody of finished goods inventory (the warehouse) should not keep the official inventory records. Accounting for finished goods inventory is performed by inventory control, an accounting function. When a single individual or department has responsibility for both asset custody and record keeping, the potential for fraud exists. Assets can be stolen or lost and the accounting records falsified to hide the event.

Objective 3. The organization should be structured so that a successful fraud requires collusion between two or more individuals with incompatible responsibilities. For example, no individual should have sufficient access to accounting records to perpetrate a fraud. Thus, journals, subsidiary ledgers, and the general ledger are maintained separately. For most people, the thought of approaching another employee with the proposal to collude in a fraud presents an insurmountable psychological barrier. The fear of rejection and subsequent disciplinary action discourages solicitations of this sort. However, when employees with incompatible responsibilities work together daily in close quarters, the resulting familiarity tends to erode this barrier. For this reason, the segregation of incompatible tasks should be physical as well as organizational. Indeed, concern about personal familiarity on the job is the justification for establishing rules prohibiting nepotism.

Supervision. Implementing adequate segregation of duties requires that a firm employ a sufficiently large number of employees. Achieving adequate segregation of

duties often presents difficulties for small organizations. Obviously, it is impossible to separate five incompatible tasks among three employees. Therefore, in small organizations or in functional areas that lack sufficient personnel, management must compensate for the absence of segregation controls with close **supervision**. For this reason, supervision is often called a compensating control.

An underlying assumption of supervision control is that the firm employs competent and trustworthy personnel. Obviously, no company could function for long on the alternative assumption that its employees are incompetent and dishonest. The competent and trustworthy employee assumption promotes supervisory efficiency. Firms can thus establish a managerial span of control whereby a single manager supervises several employees. In manual systems, maintaining a span of control tends to be straightforward because both manager and employees are at the same physical location.

Accounting Records. The **accounting records** of an organization consist of source documents, journals, and ledgers. These records capture the economic essence of transactions and provide an audit trail of economic events. The audit trail enables the auditor to trace any transaction through all phases of its processing from the initiation of the event to the financial statements. Organizations must maintain audit trails for two reasons. First, this information is needed for conducting day-to-day operations. The audit trail helps employees respond to customer inquiries by showing the current status of transactions in process. Second, the audit trail plays an essential role in the financial audit of the firm. It enables external (and internal) auditors to verify selected transactions by tracing them from the financial statements to the ledger accounts, to the journals, to the source documents, and back to their original source. For reasons of both practical expedience and legal obligation, business organizations must maintain sufficient accounting records to preserve their audit trails.

Access Control. The purpose of **access controls** is to ensure that only authorized personnel have access to the firm's assets. Unauthorized access exposes assets to misappropriation, damage, and theft. Therefore, access controls play an important role in safeguarding assets. Access to assets can be direct or indirect. Physical security devices, such as locks, safes, fences, and electronic and infrared alarm systems, control against direct access. Indirect access to assets is achieved by gaining access to the records and documents that control the use, ownership, and disposition of the asset. For example, an individual with access to all the relevant accounting records can destroy the audit trail that describes a particular sales transaction. Thus, by removing the records of the transaction, including the accounts receivable balance, the sale may never be billed and the firm will never receive payment for the items sold. The access controls needed to protect accounting records will depend on the technological characteristics of the accounting system. Indirect access control is accomplished by controlling the use of documents and records and by segregating the duties of those who must access and process these records.

Independent Verification. **Verification procedures** are independent checks of the accounting system to identify errors and misrepresentations. Verification differs from supervision because it takes place after the fact, by an individual who is not directly involved with the transaction or task being verified. Supervision takes place while the activity is being performed, by a supervisor with direct responsibility for the task. Through independent verification procedures, management can assess (1) the performance of individuals, (2) the integrity of the transaction processing system, and (3) the correctness of data contained in accounting records. Examples of independent verifications include:

- Reconciling batch totals at points during transaction processing.
- Comparing physical assets with accounting records.

- Reconciling subsidiary accounts with control accounts.
- Reviewing management reports (both computer and manually generated) that summarize business activity.

The timing of verification depends on the technology employed in the accounting system and the task under review. Verifications may occur several times an hour or several times a day. In some cases, verification may occur daily, weekly, monthly, or annually.

IT Controls

Information technology drives the financial reporting processes of modern organizations. Automated systems initiate, authorize, record, and report the effects of financial transactions. As such, they are inextricable elements of the financial reporting processes considered by SOX and need to be controlled. COSO identifies two broad groupings of IT controls: *application controls* and *general controls*. The objectives of **application controls** are to ensure the validity, completeness, and accuracy of financial transactions. These controls are designed to be application-specific. Examples include:

- A cash disbursements batch balancing routine that verifies that the total payments to vendors reconciles with the total postings to the accounts payable subsidiary ledger.
- An account receivable check digit procedure that validates customer account numbers on sales transactions.
- A payroll system limit check that identifies and flags employee time card records with reported hours worked in excess of the predetermined normal limit.

These examples illustrate how application controls have a direct impact on the integrity of data that make their way through various transaction processing systems and into the financial reporting process.

The second broad group of controls defined by the COSO framework is **general controls**. They are so named because they are not application-specific but, rather, apply to all systems. General controls have other names in other frameworks, including **general computer controls** and **information technology controls**. Whatever name is used, they include controls over IT governance, IT infrastructure, security and access to operating systems and databases, application acquisition and development, and program change procedures.

Although general controls do not control specific transactions, they have an effect on transaction integrity. For example, consider an organization with poor database security controls. In such a situation, even data processed by systems with adequate built-in application controls may be at risk. An individual who is able to circumvent database security (either directly or via a malicious program) may then change, steal, or corrupt stored transaction data. Thus, general controls are needed to support the functioning of application controls, and both are needed to ensure accurate financial reporting.

Audit Implications of SOX

Prior to the passage of SOX, external auditors were not required to test internal controls as part of their attest function. They were required to be familiar with the client organization's internal controls, but had the option of not relying on them and thus not performing tests of controls. Therefore the audit could, and often did, consist primarily of substantive tests.

SOX legislation dramatically expands the role of external auditors by mandating that they attest to the quality of their client organizations' internal controls. This constitutes the issuance of a separate audit opinion on the internal controls in addition to the opinion on

the fairness of the financial statements. The standard for this new audit opinion is high. Indeed, the auditor is precluded from issuing an unqualified opinion if only one material weakness in internal control is detected. Interestingly, auditors are permitted to simultaneously render a qualified opinion on internal controls and an unqualified opinion on the financial statements. In other words, it is technically possible for auditors to find internal controls over financial reporting to be weak, but conclude through substantive tests that the weaknesses did not cause the financial statements to be materially misrepresented.

As part of the new attestation responsibility, PCAOB Standard No. 5 specifically requires auditors to understand transaction flows, including the controls pertaining to how transactions are initiated, authorized, recorded, and reported. This involves first selecting the financial accounts that have material implications for financial reporting. Then, auditors need to identify the application controls related to those accounts. As previously noted the reliability of application controls rests on the effectiveness of the general controls that support them. Figure 1.6 illustrates this IT control relationship. The sum of these controls, both application and general, constitutes the relevant IT controls over financial reporting that auditors need to review.

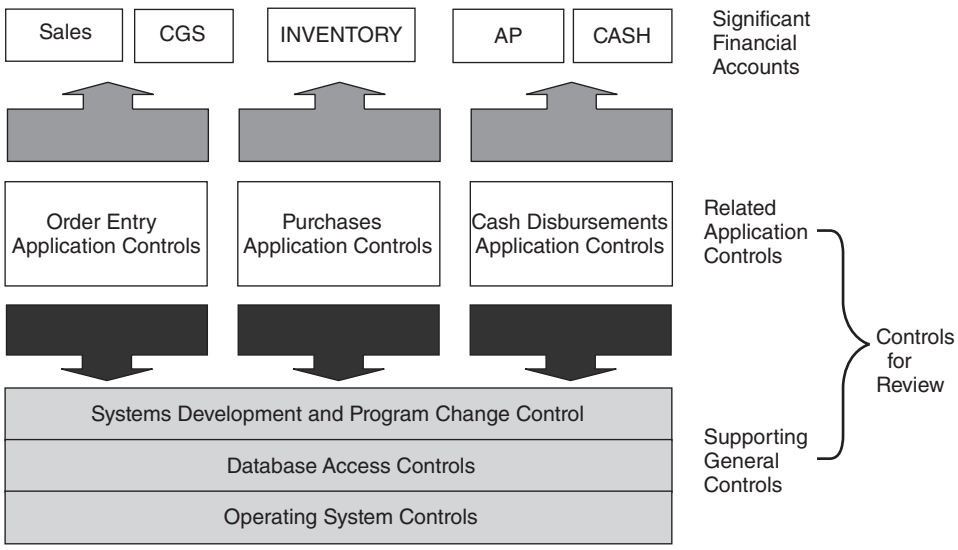
This book deals systematically with this substantial body of control and audit material. Chapters 2, 3, 4, and 5 address respectively the general control areas of IT governance, operating system and network security, database security, and systems development and program change procedures. Applications, and the design and audit of application controls are the subjects of Chapters 6, 7, 8, 9, 10, and 11.

Finally, SOX places responsibility on auditors to detect fraudulent activity and emphasizes the importance of controls designed to prevent or detect fraud that could lead to material misstatement of the financial statements. Management is responsible for implementing such controls, and auditors are expressly required to test them. Because computers lie at the heart of the modern organizations' accounting and financial reporting systems, the topic of **computer fraud** falls within the management and audit responsibilities imposed by SOX. Fraud drivers, fraud schemes, and fraud detection techniques are covered in Chapter 12.

With this backdrop in place, the scene is set for viewing control techniques and tests of controls that might be required under SOX. PCAOB Auditing Standard No. 5

FIGURE 1.6

Information Technology Control Relationship



emphasizes that management and auditors use a risk-based approach rather than a one-size-fits-all approach in the design and assessment of controls. In other words, the size and complexity of the organization needs to be considered in determining the nature and extent of controls that are necessary. The reader should recognize, therefore, that the controls and audit procedures presented in the chapters that follow describe the needs of a generic organization and may not apply in specific situations.

SUMMARY

This chapter provided an overview of IT auditing and a backdrop for the remainder of the book. We began by describing the various types of audits and distinguishing between the auditor's traditional attestation responsibility and the emerging field of advisory services. The structure of an IT audit, management assertions, audit objectives, tests of controls, and substantive tests were explained. The chapter also outlined the key points of the COSO control framework, which defines internal controls in both manual and IT environments. The final section of the chapter examined audit issues and implications related to Sarbanes–Oxley legislation and provided a conceptual framework that links general controls, application controls, and financial data integrity. The remainder of the text is based upon this framework.

KEY TERMS

access controls
accounting record
advisory services
application controls
attest service
audit objective
audit opinion
audit planning
audit procedure
audit risk
auditing
completeness
Computer-Assisted Audit Tools and Techniques (CAATTs)
control activities
control environment
computer fraud
control risk
corrective controls
Committee of Sponsoring Organizations (COSO)
data processing
detection risk
detective controls
existence or occurrence
Foreign Corrupt Practices Act of 1977 (FCPA)
general controls
general computer controls
independence
information technology controls
information technology (IT)
inherent risk
internal auditing
internal control system
limitations
management assertion
monitoring
PDC control model
presentation and disclosure
preventive controls
reasonable assurance
rights and obligations
risk assessment
Sarbanes–Oxley Act 2002
segregation of duties
Statement on Auditing Standards No. 109 (SAS 109)
substantive test
supervision
tests of controls
transaction authorization
valuation or allocation
verification procedure

REVIEW QUESTIONS

1. What is the purpose of an IT audit?
2. Discuss the concept of independence within the context of a financial audit. How is independence different for internal auditors?
3. What are the conceptual phases of an audit? How do they differ between general auditing and IT auditing?
4. Distinguish between internal and external auditors.
5. What are the four primary elements described in the definition of auditing?
6. Explain the concept of materiality.
7. How does the Sarbanes–Oxley Act of 2002 affect management's responsibility for internal controls?
8. What are the four broad objectives of internal control?
9. What are the four modifying assumptions that guide designers and auditors of internal control systems?
10. Give an example of a preventive control.
11. Give an example of a detective control.
12. Give an example of a corrective control.
13. What are the five internal control components described in the COSO framework?
14. What are the six broad classes of control activities defined by COSO?
15. Give an example of independent verification.
16. Differentiate between general and application controls. Give two examples of each.
17. Distinguish between tests of controls and substantive testing.
18. Define audit risk.
19. Distinguish between errors and irregularities. Which do you think concern auditors the most?
20. Distinguish between inherent risk and control risk. How do internal controls affect inherent risk and control risk, if at all? What is the role of detection risk?
21. What is the relationship between tests of controls and substantive tests?
22. SOX contains many sections. Which sections does this chapter focus on?
23. What control framework does the PCAOB recommend?
24. COSO identifies two broad groupings of information system controls. What are they?
25. What are the objectives of application controls?
26. Give three examples of application controls.
27. Define general controls.
28. What is the meaning of the term *attest services*?
29. List four general control areas.

DISCUSSION QUESTIONS

1. Discuss the differences between the attest function and advisory services.
2. A CPA firm has many clients. For some of its clients, it relies very heavily on the work of the internal auditors, while for others it does not. The amount of reliance affects the fees charged. How can the CPA firm justify the apparent inconsistency of fees charged in a competitive marketplace?
3. Accounting firms are very concerned that their employees have excellent communication skills, both oral and written. Explain why this requirement is so important by giving examples of where these skills would be necessary in each of the three phases of an audit.
4. Explain the audit objectives of existence or occurrence, completeness, rights and obligations, valuation or allocation, and presentation and disclosure.
5. How has the Foreign Corrupt Practices Act of 1977 had a significant impact on organization management?
6. Discuss the concept of exposure and explain why firms may tolerate some exposure.
7. If detective controls signal errors, why should they not automatically make a correction to the identified error? Why are separate corrective controls necessary?
8. Most accounting firms allow married employees to work for the firm. However, they do not allow an employee to remain working for them if he or she marries an employee of one of their auditing clients. Why do you think this policy exists?
9. In situations where unavoidable incompatible tasks are performed by employees, discuss whether the organization should rely on general authority or specific authority.

10. An organization's internal audit department is usually considered to be an effective control mechanism for evaluating the organization's internal control structure. The Birch Company's internal auditing function reports directly to the controller. Comment on the effectiveness of this organizational structure.
11. According to COSO, the proper segregation of functions is an effective internal control procedure. Comment on the exposure (if any) caused by combining the tasks of paycheck preparation and distribution to employees.
12. Discuss the key features of Section 302 of SOX.
13. Discuss the key features of Section 404 of SOX.
14. Section 404 requires management to make a statement identifying the control framework used to conduct its assessment of internal controls. Discuss the options in selecting a control framework.
15. Explain how general controls impact transaction integrity and the financial reporting process.
16. Prior to SOX, external auditors were required to be familiar with the client organization's internal controls, but not test them. Explain.
17. Does a qualified opinion on management's assessment of internal controls over the financial reporting system necessitate a qualified opinion on the financial statements? Explain.
18. The PCAOB Standard No. 5 specifically requires auditors to understand transaction flows in designing their tests of controls. What steps does this entail?
19. What fraud detection responsibilities (if any) does SOX impose on auditors?

MULTIPLE-CHOICE QUESTIONS

1. Which of the following is NOT a task performed in the audit planning phase?
   a. reviewing an organization's policies and practices
   b. planning substantive testing procedures
   c. reviewing general controls
   d. determining the degree of reliance on controls
2. Which of the following statements is true?
   a. Both the SEC and the PCAOB require the use of the COSO framework.
   b. Any framework can be used that encompasses all of COSO's general themes.
   c. The SEC recommends COBIT, and the PCAOB recommends COSO.
   d. Both the SEC and the PCAOB require the COBIT framework.
   e. None of the above are true.
3. Which of the following is NOT requirement of Section 302 of SOX?
   a. Corporate management (including the CEO) must certify monthly and annually their organization's internal controls over financial reporting.
   b. Auditors must interview management regarding significant changes in the design or operation of internal control that occurred since the last audit.
   c. Auditors must determine whether changes in internal control have materially affected, or are likely to materially affect, internal control over financial reporting.
   d. Management must disclose any material changes in the company's internal controls that have occurred during the most recent fiscal quarter.
   e. All of the above are requirements.
4. Which of the following is NOT an example of preventive control?
   a. separation of responsibilities for the recording, custodial, and authorization functions
   b. sound personnel practices
   c. documentation of policies and procedures
   d. password authentication software and hardware
   e. source documents for capturing sales data
5. The underlying assumption of reasonable assurance regarding implementation of internal control means that
   a. auditors are reasonably assured that fraud has not occurred in the period.
   b. auditors are reasonably assured that employee carelessness can weaken an internal control structure.
   c. implementation of the control procedure should not have a significant adverse effect on efficiency or profitability.
   d. management assertions about control effectiveness should provide auditors with reasonable assurance.

e. a control applies reasonably well to all forms of computer technology.

6. Ensuring that all material transactions processed by the information system are valid and in accordance with management's objectives is an example of
   a. transaction authorization.
   b. supervision.
   c. accounting records.
   d. independent verification.
7. Which of the following situations is NOT a segregation of duties violation?
   a. The treasurer has the authority to sign checks but gives the signature block to the assistant treasurer to run the check-signing machine.
   b. The warehouse clerk, who has custodial responsibility over inventory in the warehouse, selects the vendor and authorizes purchases when inventories are low.
   c. The sales manager has the responsibility to approve credit and the authority to write-off accounts.
   d. The department time clerk is given the undistributed payroll checks to mail to absent employees.
   e. The accounting clerk who shares the record-keeping responsibility for the accounts receivable subsidiary ledger performs the monthly reconciliation of the subsidiary ledger and the control account.
8. Which of the following is often called a compensating control?
   a. transaction authorization
   b. supervision
   c. accounting records
   d. segregation of duties
9. Which of the following benefits is least likely to result from a system of internal controls?
   a. reduction of cost of an external audit
   b. prevention of employee collusion to commit fraud
   c. availability of reliable data for decision-making purposes
   d. some assurance of compliance with the Foreign Corrupt Practices Act of 1977
   e. some assurance that important documents and records are protected
10. Which is NOT a source of evidence for an external auditor?
    a. work performed by internal auditors who organizationally report to the controller
    b. tests of controls
    c. substantive tests
    d. work performed by internal auditors who report to the audit committee of the BOD

PROBLEMS

1. Segregation of Functions

Comment on the specific risks (if any) that are caused by the following combination of tasks.

a. A sales manager, who works on commission based on gross sales, approves credit and has the authority to write off uncollectible accounts.
b. The warehouse clerk, who has custodial responsibility over inventory in the warehouse, updates the inventory subsidiary ledger and prepares an inventory summary for the general ledger department.
c. The billing clerk bills customers and records sales in the sales journal.
d. The shop foreman approves and submits time cards to timekeeping and distributes paychecks to employees.
e. The accounting clerk posts to individual account receivable subsidiary accounts and performs the reconciliation of the subsidiary ledger and the general ledger control account.

2. Segregation of Duties

Explain why each of the following combinations of tasks should, or should not, be separated to achieve adequate internal control.

a. Recording cash receipts in the journal and posting to the account receivable subsidiary ledger.
b. Preparation of accounts payable and distribution of payroll checks to employees (paymaster).
c. Posting of amounts from both the cash receipts and the cash disbursements journals to the general ledger.
d. Distribution of payroll checks to employees and approval of time cards.
e. Approval of bad debt write-offs and the reconciliation of accounts payable subsidiary ledger and the general ledger control account.

3. Role of Internal Audit Function

Nano Circuits Inc. is a publicly traded company that produces electronic control circuits, which are used in many products. In an effort to comply with SOX, Nano is in the process of establishing an in-house internal audit function, which previously had been outsourced. The company began this process by hiring a Director of Internal Audits. Nano Circuits' CEO recently called a planning meeting to discuss the roles of key corporate participants regarding the implementation and maintenance of internal controls. Central to this decision is the organizational placement of the future internal audit function and to whom the new Director of Internal Audit should report. In addition, Nano Circuits considered the need to reconstitute its Board of Directors Audit Committee. Participants at the meeting included the company president, the chief financial officer, a member of the audit committee, a partner from Nano Circuits external audit firm, and the Director of Internal Audits. Expectations and concerns presented by the meeting participants are summarized next.

CEO: The CEO expressed concern that Nano Circuits complies with SOX and PCAOB requirements and recommendations. The internal audit function should strengthen the organization's internal control system by developing control policies and procedures and by detecting violations of policies and procedures.

CFO: The CFO saw the role of the internal audit function as one that should be focused primarily on financial issues and therefore, the director of Internal Audits should report to the CFO.

Audit committee member: The committee member felt strongly that the Audit Committee as currently constituted is appropriate and no changes need to be made. Although none of the committee members are trained accountants they all have extensive industry experience, they have all been associated with Nano Circuits in various capacities for many years, and are well qualified to fulfill their policy-oversight responsibilities.

External audit partner: The external audit partner pointed out that the internal audit function should be organized such that it supports a close working relationship with the external auditors. This would include monitoring internal control systems on a continuing basis to provide a body of evidence on which the external auditor can rely.

Director of Internal Audits: The Director of Internal Audits argued that the new IA function should focus more on operational auditing issues, but it also should play a role in the review of internal controls over financial reporting.

Required:

a. Describe the role that each of the following areas has in the establishment, maintenance, and evaluation of internal control:
   i. Management
   ii. External auditor
   iii. Internal audit

b. To whom should the Director of Internal Audits report. Explain your answer.

c. Comment on the audit committee member's perspective as to the committee's current composition.

4. Internal Auditor Independence

Technical Solutions, Inc. is expanding and reorganizing its IA function. Currently the Director of Internal Audit, Sharon Kalafut, reports to the corporate controller, who receives and reviews all internal audit reports. Kalafut forwards copies of the internal audit reports to the audit committee of the board of directors and to the manager directly responsible for the function being audited.

An issue of contention among the management team pertains to which department or function the Director of Internal Audits should report. Martin Stevens the CEO wants to ensure that Technical Solutions complies with the SOX and that the internal audit department is structured such that it strengthens the company's internal control system. Also, an overarching objective for the reorganized audit function is that the external auditors are able to rely on the work performed by the internal audit department to a substantial degree. Arguments put forth by interested parties as to where the IA department should be organizationally located are presented next:

- **Chief Operations Officer (COO)**. John Sweeney, the COO of Technical Solutions, believes that the Director of IA should report to him. Under this arrangement the IA staff members would be involved in the preparation of policy statements on internal control regarding safeguarding of assets and in the design of business processes.
- **Chief Information Officer (CIO)**. Larry Rich, the CIO, has pushed hard to have the IA function report to him and take on an active role in the design, installation, and initial operation of a new computerized systems. IA staff will be primarily concerned with the design and implementation of internal accounting controls and conduct the evaluation of these controls during the test runs and audits.
- **Corporate Controller**. The controller, Linda Johnson, believes the IA group should remain within her functional area. Currently the IA staff performs a number of controller related tasks. These include:
  - Internal auditors reconcile bank statements of the corporation each month. The controller believes this strengthens the internal control function because the internal auditor is not

involved in either the receipt or the disbursement of cash.
- Internal auditors review the annual budget each year for relevance and reasonableness before the budget is approved. At the end of each month, the controller's staff analyzes the variances from budget and prepares explanations of these variances. These variances and explanations are then reviewed by the internal audit staff.
- Finally, the internal auditors make accounting entries for complex transactions when employees of the accounting department are not adequately trained to handle such transactions. The controller believes this gives an added measure of assurance to the accurate recording of such transactions.

Required:

a. Define independence as it relates to the internal audit function.
b. For each of the proposed tasks to be performed by the IA function, explain whether Technical Solutions' internal audit independence will be materially impaired. Consider each manager's arguments independently.
c. To maintain independence, where should the Director of Internal Audits report? Explain your answer.

5. Assessing Internal Control

The following describes the cash receipts procedures for a medium-sized online and catalogue-based retailer.

Customer payments come directly to the general mailroom along with other mail items. The customer payments mail constitutes about 20 percent of the total mail received each day. The mailroom clerks sort through the mail, open the customer payment envelopes, remove the customer checks and remittance advices, and reconcile the two documents. The mailroom supervisor then sends the reconciled checks and remittance advices to the Accounts Receivable clerk, who posts the amounts received to the customer AR subsidiary ledger and the cash receipts journal from her computer terminal. The AR clerk then manually prepares a remittance list of all checks received, endorses the checks "for deposit only" and sends the checks and remittance list to the Treasurer. Finally, the clerk files the remittance advices in the AR department.

Once the checks and remittance list arrive at the Treasury department, the treasurer reconciles the documents, and manually prepares three hard copies of the deposit slip. Next, he sends the checks and two copies of the deposit slip to the bank. Finally, he files the third copy of the deposit slip and the remittance in the department.

Required:

a. Identify the internal control weaknesses in the cash receipts process.
b. For each weakness, describe the associated risks.
c. For each weakness provide a possible control activity.

6. Assessing Internal Control

The following describes the cash disbursement procedures for a wholesale building supply company.

When the accounts payable clerk receives the supplier's invoice she records the purchase in the purchases journal, records the liability in the AP subsidiary ledger, and sets a due date based on the terms specified on the invoice. The clerk then updates the inventory control and accounts payable control accounts in the general ledger. The invoice is then filed in the department.

Each day, the clerk visually searches the AP subsidiary ledger from her terminal for invoices that are due to be paid. From her computer terminal, the clerk prepares the check and records it in the check register. The negotiable portion of the check is mailed to the vendor and a check copy is filed. The clerk then closes the liability in the AP subsidiary ledger and updates the accounts payable control and cash accounts in the general ledger.

Required:

a. Identify the internal control weaknesses in the cash disbursement process.
b. For each weakness, describe the associated risks.
c. For each weakness, provide a possible control activity.

7. Evaluation of Controls

Gaurav Mirchandaniis is the warehouse manager for a large office supply wholesaler. Mirchandaniis receives two copies of the customer sales order from the sales department. He selects the goods from the shelves and sends them and one copy of the sales order to the shipping department. He then files the second copy in a temporary file. At the end of the day, Mirchandaniis retrieves the sales orders from the temporary file and updates the inventory subsidiary ledger from a terminal in his office. At that time, he identifies items that have fallen to low levels, selects a supplier, and prepares three copies of a purchase order. One copy is sent to the supplier, one is sent to the accounts payable clerk, and one is filed in the warehouse. When the goods arrive from the supplier, Mirchandaniis reviews the attached packing slip, counts and inspects the goods, places them on the shelves, and updates the inventory ledger to reflect the receipt. He then prepares a receiving report and sends it to the accounts payable department.

Required:

a. Prepare a systems flowchart of the procedures previously described.
b. Identify any control problems in the system.
c. What sorts of fraud are possible in this system?

8. Evaluation of Controls

Matt Demko is the loading dock supervisor for a dry cement packaging company. His work crew is composed of unskilled workers who load large transport trucks with bags of cement, gravel, and sand. The work is hard, and the employee turnover rate is high. Employees record their attendance on separate time cards. Demko authorizes payroll payments each week by signing the time cards and submitting them to the payroll department. Payroll then prepares the paychecks and gives them to Demko, who distributes them to his work crew.

Required:

a. Prepare a systems flowchart of the procedures described here.
b. Identify any control problems in the system.
c. What sorts of fraud are possible in this system?

CHAPTER 2

Auditing IT Governance Controls

LEARNING OBJECTIVES

After studying this chapter, you should:

- Understand the risks of incompatible functions and how to structure the IT function.
- Be familiar with the controls and precautions required to ensure the security of an organization's computer facilities.
- Understand the key elements of a disaster recovery plan.
- Be familiar with the benefits, risks, and audit issues related to IT outsourcing.

This chapter presents risks, controls, and tests of controls related to IT governance. It opens by defining IT governance and the elements of IT governance that have internal control and financial reporting implications. First, it presents the exposures that can arise from inappropriate structuring of the IT function. Next, the chapter reviews computer center threats and controls, which include protecting it from damage and destruction from natural disasters, fire, temperature, and humidity. The chapter then presents the key elements of a disaster recovery plan, including providing second-site backup, identifying critical applications, performing backup and off-site storage procedures, creating a disaster recovery team, and testing the plan. The final section of the chapter presents issues concerning the growing trend toward IT outsourcing. The logic behind management decisions to outsource is explored. The chapter also reveals the expected benefits and the risks associated with outsourcing. The chapter concludes with a discussion of audit issues in an outsourcing environment and the role of the SAS 70 report.

INFORMATION TECHNOLOGY GOVERNANCE

Information technology (IT) governance is a relatively new subset of corporate governance that focuses on the management and assessment of strategic IT resources. The key objectives of IT governance are to reduce risk and ensure that investments in IT resources add value to the corporation. Prior to the Sarbanes–Oxley (SOX) Act, the common practice regarding IT investments was to defer all decisions to corporate IT professionals. Modern IT governance, however, follows the philosophy that all corporate stakeholders, including boards of directors, top management, and departmental users (i.e., accounting and finance) be active participants in key IT decisions. Such broad-based involvement reduces risk and increases the likelihood that IT decisions will be in compliance with user needs, corporate policies, strategic initiatives, and internal control requirements under SOX.

IT Governance Controls

Although all IT governance issues are important to the organization, not all of them are matters of internal control under SOX that may potentially impact the financial reporting process. In this chapter, we consider three IT governance issues that are addressed by SOX and the COSO internal control framework. These are:

1. Organizational structure of the IT function
2. Computer center operations
3. Disaster recovery planning

The discussion on each of these governance issues begins with an explanation of the nature of risk and a description of the controls needed to mitigate the risk. Then, the audit objectives are presented, which establishes what needs to be verified regarding the function of the control(s) in place. Finally, example tests of controls are offered that describe how auditors might gather evidence to satisfy the audit objectives. These tests may be performed by external auditors as part of their attest service or by internal auditors (or advisory services professionals) who are providing evidence of management's compliance with SOX. In this regard, we make no distinction between the two types of services.

STRUCTURE OF THE CORPORATE IT FUNCTION

The organization of the IT function has implications for the nature and effectiveness of internal controls, which, in turn, has implications for the audit. In this section, some important control issues related to IT structure are examined. These are illustrated through two extreme organizational models—the centralized approach and the distributed approach. The risks, controls, and audit issues related to each model are then discussed. The reader should recognize, however, that most organizational structures embody elements of both models.

Centralized Data Processing

Under the **centralized data processing** model, all data processing is performed by one or more large computers housed at a central site that serves users throughout the organization. Figure 2.1 illustrates this approach, in which IT services activities are consolidated

and managed as a shared organization resource. End users compete for these resources on the basis of need. The IT services function is usually treated as a cost center whose operating costs are charged back to the end users. Figure 2.2 illustrates a centralized IT services structure and shows its primary service areas: database administration, data processing, and systems development and maintenance. A description of the key functions of each of these areas follows.

FIGURE 2.1

Centralized Data Processing Approach

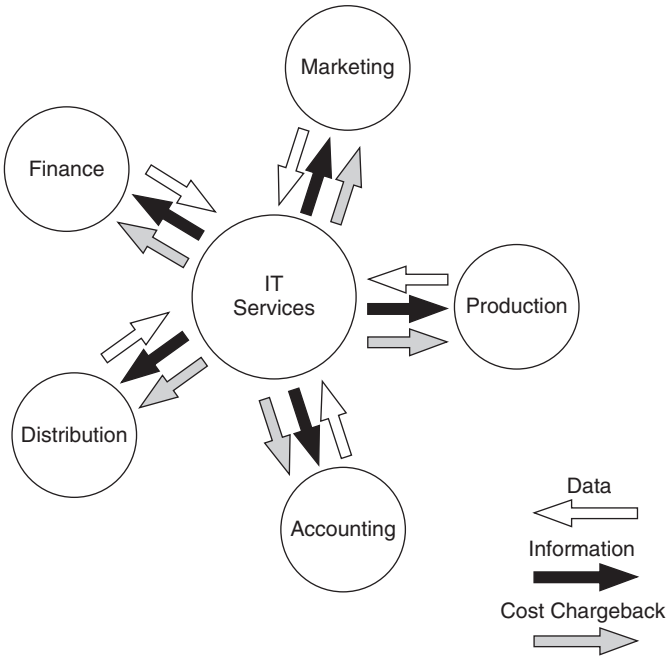
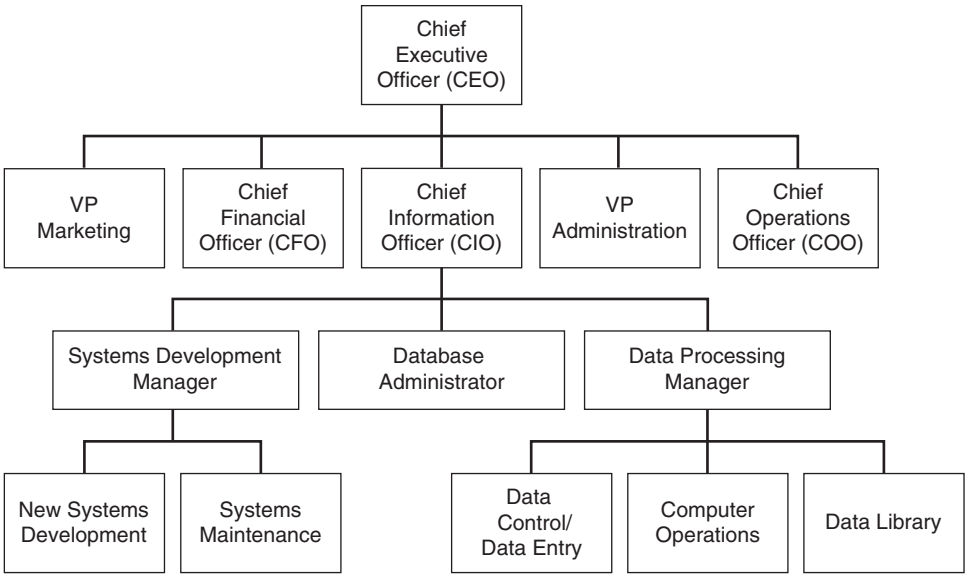


FIGURE 2.2

Organizational Chart of a Centralized IT Services Function



Database Administration

Centrally organized companies maintain their data resources in a central location that is shared by all end users. In this shared data arrangement, an independent group headed by the database administrator (DBA) is responsible for the security and integrity of the database.

Data Processing

The data processing group manages the computer resources used to perform the day-to-day processing of transactions. It consists of the following organizational functions: **data control/data entry**, **computer operations**, and the **data library**.

Data Control/Data Entry. The data control/data entry function receives hard copy source documents from end users and transcribes these into digital format for computer processing in batch systems. For example, data control/entry would keystroke sales order data onto magnetic disks for input into the system. After data processing this group would then disseminate the finished sales reports to the appropriate end users, such as the marketing manager.

Computer Operations. The electronic files produced in data conversion are later processed by the central computer, which is managed by the computer operations groups. Accounting applications are usually executed according to a strict schedule that is controlled by the central computer's operating system.

Data Library. The data library is a room adjacent to the computer center that provides safe storage for the off-line data files. Those files could be backups or current data files. For instance, the data library could be used to store backup data on DVDs, CD-ROMs, tapes, or other storage devices. It could also be used to store current operational data files on magnetic tapes and removable disk packs. In addition, the data library is used to store original copies of commercial software and their licenses for safekeeping. A data librarian, who is responsible for the receipt, storage, retrieval, and custody of data files, controls access to the library. The librarian issues data files to computer operators in accordance with program requests and takes custody of files when processing or backup procedures are completed. The trend in recent years toward real-time processing and the increased use of direct-access files has reduced or even eliminated the role of the data librarian in many organizations.

Systems Development and Maintenance

The information systems needs of users are met by two related functions: system development and systems maintenance. The former group is responsible for analyzing user needs and for designing new systems to satisfy those needs. The participants in system development activities include systems professionals, end users, and stakeholders.

Systems professionals include systems analysts, database designers, and programmers who design and build the system. Systems professionals gather facts about the user's problem, analyze the facts, and formulate a solution. The product of their efforts is a new information system.

End users are those for whom the system is built. They are the managers who receive reports from the system and the operations personnel who work directly with the system as part of their daily responsibilities.

Stakeholders are individuals inside or outside the firm who have an interest in the system, but are not end users. They include accountants, internal auditors, external auditors, and others who oversee systems development.

Once a new system has been designed and implemented, the systems maintenance group assumes responsibility for keeping it current with user needs. The term *maintenance* refers to making changes to program logic to accommodate shifts in user needs over time. During the course of the system's life (often several years), as much as 80 or 90 percent of its total cost may be incurred through maintenance activities.

Segregation of Incompatible IT Functions

The previous chapter stressed the importance of segregating incompatible duties within manual activities. Specifically, operational tasks should be segregated to:

1. Separate transaction authorization from transaction processing.
2. Separate record keeping from asset custody.
3. Divide transaction-processing tasks among individuals such that short of collusion between two or more individuals fraud would not be possible.

The IT environment tends to consolidate activities. A single application may authorize, process, and record all aspects of a transaction. Thus, the focus of segregation control shifts from the operational level (transaction processing tasks that computers now perform) to higher-level organizational relationships within the computer services function. Using the organizational chart in Figure 2.2 as a reference, the interrelationships among systems development, systems maintenance, database administration, and computer operations activities are examined next.

Separating Systems Development from Computer Operations

The segregation of systems development (both new systems development and maintenance) and operations activities is of the greatest importance. The relationship between these groups should be extremely formal, and their responsibilities should not be commingled. Systems development and maintenance professionals should create (and maintain) systems for users, and should have no involvement in entering data, or running applications (i.e., computer operations). Operations staff should run these systems and have no involvement in their design. These functions are inherently incompatible, and consolidating them invites errors and fraud. With detailed knowledge of the application's logic and control parameters and access to the computer's operating system and utilities, an individual could make unauthorized changes to the application during its execution. Such changes may be temporary ("on the fly") and will disappear without a trace when the application terminates.

Separating Database Administration from Other Functions

Another important organizational control is the segregation of the DBA from other computer center functions. The DBA function is responsible for a number of critical tasks pertaining to database security, including creating the database schema and user views, assigning database access authority to users, monitoring database usage, and planning for future expansion.[1] Delegating these responsibilities to others who perform incompatible tasks threatens database integrity. Thus, we see from Figure 2.2 how the DBA function is organizationally independent of operations, systems development, and maintenance.

1 The role of the DBA is examined in more detail in Chapter 4.