CHAPTER ONE

Why Is IT Auditing Important to the Financial Auditor and the Financial Statement Audit?

MANY FINANCIAL AUDITORS BELIEVE THAT complex IT environments require a technically trained professional to fully comprehend the technologies employed in the environment. Other financial auditors may decide to rescope the audit (if a non-Sarbanes-Oxley [SOx] engagement) in order to avoid looking at internal controls, or at least the IT controls, while yet others may perform a superficial, high-level review of the IT controls and hope no one notices that it was not very detailed.

Anything that a client provides that is not manually created relies on IT for the accounting process, and you must understand how to test the IT systems and whether to rely on it. By appropriately assessing the IT controls, you may be able to reduce the overall effort of the audit, and bring new observations to your client about the IT environment.

An effective assessment of IT controls may actually increase the amount of time required to perform an audit. However, consistent with Auditing Standards (SASs) Nos. 104–111, if you have an adequate understanding of the entity, its internal control and processes, and its environment and other factors, the cost increase will likely be less because the auditor will have a reduced learning curve. The cost to make audit methodology changes could be significant in the first year, but is likely to increase the efficiency with which you conduct your future audits, minimizing audit fee increases to the less complex clients.

It is common in academic curricula and continuing professional education to describe audits by one of four categories:

1. Internal audits
2. Financial or external audits
3. Fraud audits
4. Information technology audits

Following graduation from an accounting or equivalent program and certification as a Certified Public Accountant (CPA) or in another area (e.g., Certified Internal Auditor [CIA]), the practitioner keeps those definitions in mind. As a practical matter, these "silos" are helpful to delineate the differences between the audits, but they overwhelmingly ignore one common reality: All financial audits require the auditor to understand where the information comes from and what processes ensure its reliability. A second reality is that information technology is becoming increasing pervasive and more sophisticated.

Our philosophy of IT auditing embraces the answer to a question you may have asked: *Where does IT auditing fit into the financial auditing process?* We believe that it should fit in throughout the entire engagement. At any step in the process, when we are retrieving information for any cycle, we need to ask—and to be able to answer—questions about where the information came from and what processes ensure its reliability. In virtually all phases of the audit, the auditor must understand the answers to those questions, including the IT controls that cover a particular system or process and knowing how to test these controls in order to provide evidence that they are working properly.

MANAGEMENT'S ASSERTIONS AND THE IT AUDIT

Auditors are familiar with the concept of *management assertions*, the idea that the financial statements imply a set of claims concerning the reported amounts and balances. Each of these assertions can be associated with potential misstatements and in turn with audit procedures. In the following paragraphs we review the principal assertions and briefly expand the financial-auditing discussion to encompass related IT-auditing issues.

Existence

Many account balances purport to describe quantities that actually exist (e.g., stocks of inventory or amounts owed to the company for past sales). Over- or understatements of these balances may result in material errors, and audit procedures typically rely on a combination of process analysis and physical counts or sampling approaches to evaluate the plausibility of a reported balance. The financial auditor ties information in the system back to transaction (source) documents (which may be paper or another electronic file), and, accordingly, he or she needs to understand the system's overall design, the flow of information, and the nature and location of files.

The IT audit process goes beyond a merely conceptual understanding of these issues in order to focus on specific features of the accounting system. The IT audit must evaluate the likelihood that problems or defects in design or operation could lead to misstatements. Thus there is an IT corollary to the financial statement assertion of existence, namely that the application controls that support processing integrity exist. These include such IT-based items as access controls, proper segregation, and appropriate configurations. For instance, when an IT auditor tests for access control, we would expect the existence of signed forms with management approval that specify the access needed. When an IT auditor tests change management, we would expect to see change

control forms with the requested changes that are approved for each change that is captured in the system. In smaller organizations, this type of existence assertion can be challenging to achieve due to lack of supporting documentation.

In later chapters we examine these types of issues in specific detail for each of the major transaction cycles.

Completeness

The completeness assertion refers to the integrity of the recording process and the ability of the company's accounting system to ensure that the effects of all transactions, balances, accounts, estimates, and so on have been included in the financial statements. Traditional audit techniques such as cross-footing and internal validity checks of totals and subtotals can help to ensure that financial information flows correctly (as missing values may cause the statements and supporting schedules not to tie). At the IT level, the auditor is concerned with how the system ensures completeness—for instance, does the report writer pull all the items from the chart of accounts?

There is also an IT corollary to the completeness assertion, namely that all necessary and required controls exist. This completeness assertion differs slightly from the existence assertion: While the latter requires the IT auditor to verify that claimed controls actually exist, the former requires that he critically evaluate the overall system design and perhaps recommend additional controls or procedures. Note also that in smaller organizations it may be challenging to achieve completeness due to lack of understanding of how to determine how the accounting system pulls its data.

Rights and Obligations

This assertion addresses the legal status of a company's assets and liabilities and it can create exposures and areas of interest from an IT perspective. As an example, consider a company that ships merchandise on both a free-on-board (FOB) destination and FOB shipping point basis. The accounting system should be configured so as to properly classify these transactions and support accurate reporting of inventory, receivables, and sales.

There is also an IT corollary to the rights and obligations assertion, namely ownership of and responsibility for information resources controlled within the company's accounting system. Thus, from this perspective, adequate control over segregation of duties becomes an important part of the overall structure of rights and obligations as they affect accounting information. In some organizations, a person may have certain responsibilities that are well-controlled outside the system, but the system itself may not coordinate the necessary data access rights for employees to function effectively. Additionally, the company will usually have an obligation to protect data privacy.

Valuation

The area of valuation can range from the accuracy of original costs to complex and esoteric calculations relating to financial instruments. In order to ensure that account balances, transactions, fair value estimates, and other amounts are reported

appropriately, the IT auditor may need to examine things such as links to pricing tables and lookup tables, the design and accuracy of spreadsheet models, and the integrity of proprietary data sources. The widespread use of spreadsheet models for a variety of valuation-related activities creates many exposures related to data transfer and change management.

IT and valuation intersect when the auditor needs to estimate the potential cost exposure from an IT audit issue. For example, if an auditor determines that inappropriate individuals have access to make adjusting journal entries, the auditor should then determine if any unauthorized journal entries were actually made by examining the general ledger entries. If any are identified, then the auditor would need to value the exposure to the financial statements.

Accounting Procedures

The realm of accounting procedures includes classification and aggregation procedures, proper cutoffs at the end of each accounting period, the preparation and posting of adjusting entries, the preparation of disclosure and supporting schedules, and the final presentation of the financial statements. It also presumes the fundamental accuracy of arithmetic processes and conformity with appropriate accounting standards.

At the general financial level, the auditor may review personnel records in order to evaluate the suitability of individuals who perform these various tasks. The IT analog would include an analysis of access rights and log-on records. For instance, the IT auditor might run all the adjusting entries, check to see who posted them, and evaluate the list according to a chart of responsibilities.

In addition, the auditor should examine the configuration settings in the computer system to ensure that proper cutoff is achieved. For example, does the computer system configuration close the accounting period, or does the accounting period remain open indefinitely? Does the system have the correct days set for each month? When the financial statements are being produced, the IT auditor needs to ensure that all data within the accounting system are being pulled to the financial statements, confirming, for example, accurate tie-backs between subledgers, the general ledger, and the financial statements.

A Note on Sarbanes-Oxley

The discussion in this text does not focus on the Sarbanes-Oxley Act (SOx), in part because most SMEs do not have to comply with these provisions, and in part because there is already a significant quantity of published guidance in this area. It's worth noting, however, that many items of SOx guidance could be useful for a variety of general controls and as part of a program that addresses other company-specific control issues.

OBJECTIVES OF DATA PROCESSING FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)

There are several paradigms and methodologies for conducting IT audits. As discussed in the sidebar titled "Committee of Sponsoring Organizations," many of these focus on high-level concepts and principles that should guide the IT audit process. These paradigms share three pervasive IT objectives: the *confidentiality*, *integrity*, and *availability* (CIA) of data. From the Guide to the Assessment of IT Risk (GAIT) methodology we focus on three crucial IT domains: (1) change management, (2) operations, and (3) security.

In this section we briefly discuss CIA and then identify some crucial intersections.

1. **Confidentiality:** The confidentiality of data refers to both internal and external users. Internally, the system of rights and permissions to access and modify data is an essential building block in the design of properly segregated duties (or a key feature to analyze when insufficient personnel make it impossible to achieve an ideal level of segregation). Externally, the confidentiality of data rests on such IT constructs as firewalls, encryption, and access protocols.
2. **Integrity:** In an accounting context, data integrity relates directly to the management assertions discussed in the preceding section, and to the Conceptual Framework's notion of *representational faithfulness*. Thus, accounting information should represent what it purports to represent—quantities that actually exist, calculated from complete records, with due consideration to appropriate legal rights and obligations, and correctly valued in accordance with acceptable accounting procedures.
3. **Availability:** Data that is not available to users is by definition useless to them. Relevant IT concerns include server reliability, access controls, protocols for distributing data, and concurrency issues.

As Figure 1.1 suggests, there are crucial interconnections between these objectives. Confidentiality and integrity intersect in the design of a company's internal control system, as inadequate attention to confidentiality issues may create exposures that either

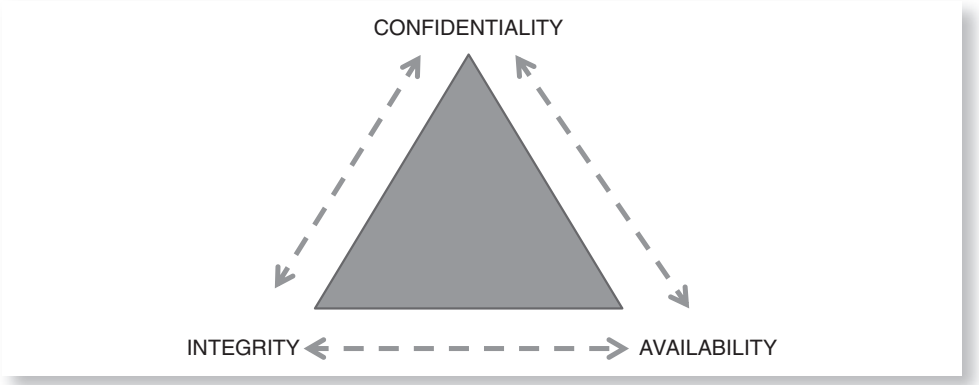

FIGURE 1.1 CIA

Committee of Sponsoring Organizations

The Committee of Sponsoring Organizations (COSO) was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that lead to fraudulent financial reporting (COSO 2013a). COSO is comprised of five organizations, including the Institute of Management Accountants, the American Accounting Association, the American Institute of Certified Public Accountants, the Institute of Internal Auditors, and Financial Executives International.The stated goal of COSO is to provide thought leadership on governance, enterprise risk management (ERM), internal controls, and fraud deterrence. The 1992 COSO report is recognized as an authoritative source on internal controls and provides a framework against which internal control systems may be assessed. In 2006, COSO issued guidance on how to apply the COSO framework to smaller public companies. Chapter 9 includes an extensive discussion of COSO's guidance for smaller public companies as many of the concepts apply to SMEs regardless of whether they are public or private.

COSO released an updated *Internal Control—Integrated Framework* in 2013 (COSO 2013b). The most current release formalizes many of the fundamental concepts introduced in the original COSO framework. The five principles of internal controls in 2013 were the five concepts of internal controls in the previous COSO release. Consistent with earlier frameworks, the 2013 principles provide the user with assistance in the design and implementation of internal controls and a framework against which internal control systems may be assessed.

Sarbanes-Oxley

In response to the series of business failures and corporate scandals that began with Enron in 2001, the U.S. Congress enacted the Sarbanes-Oxley Act of 2002 (SOx). The stated purpose of SOx is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws (Public Law 107–204 2002). There are 11 sections of SOx-defining auditor and corporate responsibilities, including expectations for financial disclosures, strong penalties for white-collar crimes, and protection for whistleblowers. Like many legislative acts, the U.S. Congress did not provide the necessary specificity for implementation. Practitioners from public accounting and companies that had to comply reached back to the 1992 COSO report as an authoritative source to produce the necessary specificity to implement SOx.

SOx also created the Public Company Accounting Oversight Board (PCAOB) to oversee the audits of public companies to protect the interests of investors and to further public interest by the preparation of accurate and independent audit reports. The PCAOB issued guidance for IT controls and thus falls within the broader topic of IT audit concerns.

COBIT

While COSO provides thought leadership on governance, ERM, internal controls, and fraud deterrence, COBIT 4.1 provides thought leadership and guidance within the IT function to address risk management, internal controls, and other relevant best practices. Chapter 10 provides an extensive discussion of COBIT 4.1 and its intersection with COSO. Chapter 10 also includes a discussion of previous PCAOB guidance and its intersection with COBIT. The intersection of COBIT with COSO is extremely important to the financial or IT auditor, given COSO's significance to risk and internal control guidelines regardless of whether the enterprise is small, large, public, or private. COBIT 5, an update of COBIT 4.1, remains very relevant to COSO as this framework shifts from an IT-centric view to an enterprise view and considers IT and its collective contribution (e.g., enterprise data) within the larger risk framework.

TABLE 1.1 IT Objectives and Domains Mapped to CIA

IT Objectives/ IT Domains	Confidentiality	Integrity	Availability
Change Management	Segregation, authorization	Accuracy and reliability of changes	Rollback procedures
Operations	Safety of backups, access to backups, access control	System restorability	Server capacity, licenses, personnel backups
Security	Permissions, log-on histories	Nature and reliability of controls	Security roles exist, passwords exist

corrupt the integrity of data or, at a minimum, raise concerns about the potential for this to happen. Confidentiality intersects with availability where the scheme of permissions and access rights is defined. Availability and integrity intersect at the point where information is required to process transactions (e.g., data from a customer's subledger account must be available when a payment is received), make estimates (e.g., receivables and collection data should be available in order to estimate credits to the valuation allowance), or prepare statements and schedules.

Table 1.1 illustrates some of the important intersections between CIA objectives and the three IT domains of change management, operations, and security. The change management process should minimize the exposures created by transition from one state to another, and ensure that the change results in a stable endpoint. Operations need to occur in a stable and secure fashion. Security is a pervasive concern.

Confidentiality

- **Change management:** Segregation refers to the well-established principle that programmers should not have access to data, and that those entrusted with data should not have programming rights. As examined in detail in later chapters, we define *programming* broadly so as to encompass the many methods of altering how software functions and the results it produces. When an IT auditor tests change management, we would expect to see change control forms with the requested changes that are approved for each change that is captured in the system.
- **Operations:** Confidentiality concerns in the operations domain include issues such as the storage location of backup tapes. There's a difference between a sock drawer and a fireproof safe! It's important to remember that the data on the backup tape is confidential and may be readily converted to useful information without someone having access to the system. With respect to access control, IT auditor tests should expect the existence of signed forms with management approval, specifying the access needed.
- **Security:** This intersection includes topics such as passwords, permissions, log-on histories (detective control), and penetration testing. The auditor should determine whether company personnel have access only to the data they need—or to more. It is important to understand and *document* the business reason for data access protocols.

Hard and Soft Controls

At the organizational level, the terms *hard control* and *soft control* refer to the dichotomy between formal and restrictive policies that represent externally imposed discipline, and the sorts of informal, shared values that promote high levels of cohesion and commitment to the unit's objectives. In the IT domain these terms have an analogous relationship to each other, but generally refer to the specific features of the software that either prevent a user from doing certain things (hard control) or warn her about specific consequences or problems (soft control).

As an example, consider an Excel template that is used for pricing. A soft control would be an error flag that produced a warning message if input values fell outside of a specified range. A hard control would be a protected sheet with pricing inputs restricted to input from a dropdown menu or a lookup table. Data entry to unprotected cells can be restricted in various ways.

Integrity

- **Change management**: The IT audit should ensure that appropriate end-user testing has occurred and that changes are working as intended and in a manner that can be relied upon.
- **Operations:** Concerns in this area include testing of backup tapes for system restorability. If data cannot be restored, the company may have incomplete records.
- **Security:** The auditor should understand whether she can rely on the system's security. Are there ways in which it could be bypassed or compromised? What are the overriding security controls? Are they soft or hard?

Availability

- **Change management:** Is the source code in a location where it can be restored? Are there rollback procedures in case of a failed change? Is the backup tape available in case management needs to access data that is not currently in the system?
- **Operations:** The IT auditor should consider the ability of the server system to handle the day-to-day load. Does management have all the needed licenses and are they current? Are there any concerns about the computer system's availability? The location and availability of backup tapes is important. How, if it were necessary, would an employee access prior-year information that is no longer kept in the system?
- **Security:** Whereas the primary security concern is unauthorized access, it's also important that the system not lock out users who have innocently lost or forgotten a password. The IT auditor should understand procedures that ensure, as well as restrict, availability.

SPECIAL CHALLENGES FACING SMEs

How a Small Business Evolves

Almost everyone has heard the story of how Steve Jobs and Steve Wozniak developed a business from a single concept that preceded the Lisa and the Macintosh and led to a

series of steps that eventually evolved into Apple Computer (Apple 1 2013). The characteristics of the first business created by Jobs and Wozniak are emblematic of many SMEs: a high concentration of ownership, a high emphasis on revenue generation and cash, a niche product, and a handful of valued employees. The working relationships were very close as familiarity bred longtime friendships and real or perceived trust. Wozniak was among the first to be interviewed following Jobs' death and described the passing of Steve Jobs as a significant loss (Metz 2011). Jobs and Wozniak sold their first "Apple 1s" to the Byte Shop in Mountain View, California, for $666 each. Apple 1s were the first single-board computers with onboard read-only memory and included a video interface—a niche product with a narrow geographical reach.

Although little documentation exists about the early stages of Apple 1, it's reasonable to speculate that bookkeeping and the associated controls were low priorities. It's unlikely a full-time, seasoned Certified Public Accountant was on the payroll to supervise and prepare the financial statements, let alone was an internal audit function established to review compliance to internal controls and assess enterprise risk. A positive cash flow versus compliance to generally accepted accounting principles (GAAP) was more likely the first priority as Steve Jobs sold a Volkswagen minibus for investment infusion into a newly found passion. The bookkeeping was probably very simple, e.g. a checkbook, and did not include Excel spreadsheets, QuickBooks, or Microsoft Dynamics as those products were not yet invented. No one was concerned whether program changes to the bookkeeping software were unauthorized or whether anyone using the software was qualified because the software didn't exist. With data captured in a checkbook, daily data backups in the office and another with more time periods in another offsite location are not required. Beyond the bookkeeping and financial reporting, what else is relevant to the internal controls for this small business?

The opportunities for management override of internal controls (assuming some controls existed) by either Steve Jobs or Steve Wozniak was a significant risk as either could have taken the proceeds of a product delivery and "disappeared." But each partner knew the operations, including product deliveries, revenue proceeds, and a sense of reasonableness. Unusual transactions would have been noticed immediately. Developing an environment in a smaller business with reduced risk requires clear objectives with an organization qualified and trained for the responsibilities. The tone at the top or at the senior management level emphasizes integrity and value systems consistent with a sound control environment. It is very likely that technical skills related to the Apple 1 were highly revered by Jobs and Wozniak with administrative and internal control skills as a distant second or even a remote priority. Competent personnel at all levels of the enterprise were something for the future, but not when they were selling personal assets to finance the business. The concepts of *IT governance* or the Committee of Sponsoring Organizations (COSO) did not exist in Steve Jobs' or many Fortune 1000 board members' vocabulary or list of priorities. Steve Jobs never lamented the role of a weak or nonexistent board of directors for the Apple 1 business. The previous three paragraphs describing Apple 1 and Steve Jobs during its early years, albeit hypothetical, are very different from the SME environment that exists today.

Although there was no evidence of fraud in the early business ventures by Jobs and Wozniak (nor are we in any way implying that fraud existed), research by the

Association of Certified Fraud Examiners (ACFE) suggests that small companies are among the most vulnerable to fraud and loss. According to a report from ACFE, *The 2012 Report to the Nation on Occupational Fraud and Abuse* (ACFE 2012), small businesses, defined as those with less than 100 employees, suffered both a greater percentage of frauds (32 percent) and a higher median loss ($147,000) than their larger counterparts. These findings accentuate the problems associated with SMEs. They are limited in the amount of financial and human resources, including trained IT personnel, to deter fraud and abuse. According to ACFE research, billing schemes, skimming, cash larceny, and payroll fraud were noticeably more common in businesses with less than 100 employees. Across all sizes of organizations and government entities, tips were the most common detection method, followed by internal controls and internal audits. Pragmatically, few if any SMEs employ internal audits and must rely on other vehicles, if any, for fraud detection. Publicly traded companies cited the smallest percentage of fraud detected by external audits even though they are the only type of organization that is required to have an external audit.

The 2012 ACFE report is reinforced with more recent experience from the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates hacking attacks (Fowler and Worthen 2011). The forensic units responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63 percent, were at companies with 100 employees or fewer. Visa Inc. estimates about 95 percent of the credit-card data breaches it discovers are on its smallest business customers. Hackers would rather spend time on SMEs and make a quick harvest than break into a Fortune 500 with substantially more effort. According to Symantec, the credit cards and bank accounts offered in the underground economy are worth more than US$7 billion.

The Control Environment for SMEs

Since Apple 1, software applications and the Internet have emerged to be significant control topics for the SME. Today, an SME would likely use Excel spreadsheets, QuickBooks, or Microsoft Dynamics with the potential of cloud applications such as Google Apps for Business. QuickBooks has an active user base of 4.5 million companies and is the world's most popular accounting software (Collins 2011). While much has changed since Apple 1 with the evolution of new software products such as QuickBooks and Microsoft Dynamics, much remains unchanged. Adequate staffing, segregation of duties, competent personnel, qualified board members, the tone at the top, and general controls are among the topics for SMEs that remain constant before and after the emergence of Excel spreadsheets, QuickBooks, or Microsoft Dynamics. While these controls remain constant, they must be adjusted for the new reality of software applications that did not exist in the previous generation of SMEs. For example, the definition of competent personnel must now include an employee who understands QuickBooks at a minimum level of proficiency. A new genre of internal controls described as *IT controls* has emerged with a reliance on the new software technology.

Adequate staffing to support segregation of duties is an ongoing concern with SMEs. The person who opens the mail and logs payments should not be the same person who makes deposits and maintains the bookkeeping records. Additional segregations of duties

should be in place: Receipts should be offered to all customers with the requirement that subsequent transactions be accompanied by a receipt; excessive voided sales should be investigated; all credit memos and write-offs should require management approval; and management should investigate customer complaints about unusual balances (Raimondi 2011). Segregation of duties is also important for cash disbursements: A review of the original invoice should be made prior to payment; purchase orders should be used for all significant purchases; the purchase orders should use an approved vendors' list (management approves the list of approved vendors); the check signor should not be the bookkeeper; all online payments are approved by a second person; and one person controls payments while a second person controls blank checks and monitors check numbers. Additional areas that should require segregation of duties include payroll reviews, fixed asset inventories and reviews, and bank credit card activities. Has anything else changed as a result of QuickBooks, Microsoft Dynamics, and Excel in the SME? Management and auditors alike need to reflect on this question in order to ensure that all risks and controls have been considered.

The need for general, often physical, controls outside of the IT environment, including locked doors, cash registers, offices, file cabinets, and control of blank checks, has changed little with the emergence of QuickBooks, Microsoft Dynamics, and Excel. Within the IT environment, the emergence of server cabinets and backup files has increased the need for greater security for servers (and backup servers) and offsite storage of files. Wireless access to the SME network should include the appropriate encryption (e.g., WiFi-protected access [WPA2] or a more recent product). With software on servers and Internet availability, restricted access through passwords and the appropriate implementation of firewalls and ongoing file backups should be normal protocol. Background checks and security cameras should be implemented wherever appropriate and particularly where high-value inventory exists. A broader discussion of general controls for SMEs occurs later in this book.

Significant application controls for Excel, Microsoft Dynamics, and QuickBooks include access controls, closing dates, a variety of reports validating the data, budgetary controls, customer credit card protection, and user preferences. In this chapter, we introduce application topics for further review in more detail in later chapters. In QuickBooks, user names and passwords can be administered for sales and accounts receivable, purchases and accounts payable, checking and credit cards, inventory, time tracking, payroll and employees, sensitive accounting activities, sensitive financial reports, changing or deleting transactions, and changing closed transactions. In the QuickBooks Enterprise Solution, customization to enable application control fine tuning includes predefined roles, individual reports, bank accounts, lists, and activities with the ability to customize each user's access to view-only, create, modify, delete, and print. Controlling transactions in closed periods is particularly important to the integrity of financial reporting. In QuickBooks, the closing date password can be established with the ability to restrict access to prior periods. A closing date exception report is available for management review. Additional application controls include reports for the audit trail, voided/deleted transactions, previous reconciliation, discrepancy, closing date, and exception report. Additional application controls will be reviewed in later chapters.

The Board's and Management's Roles in the SME Control Environment

According to the SEC's Office of Economic Analysis, insiders own on average approximately 30 percent of the company's shares (GAO 2006) for those public companies with a market capitalization of $125 million or less. With the high concentration of ownership in smaller public companies, the same need for significant investor SEC protection in a Fortune 1000 company with broad stock ownership does not exist. However, while there is some benefit in concentrated management and ownership, there are also extensive and numerous risks, including management override of internal controls.

While the risk of management override exists with a concentration of management and ownership, greater oversight, exposure, and transparency of the business can also evolve from a smaller company, provided senior management creates the leadership for those characteristics to evolve. Steve Jobs and Steve Wozniak were hands-on during the evolution of Apple 1 and were very aware of product movement, product costs, and administrative expenses. Achieving and evaluating effective internal controls over financial reporting can be simplified if management maintains hands-on involvement and awareness of sales, costs, and administrative expenses.

SME shareholders, the board, managers, and audit committees (if an audit committee exists) should actively (and periodically) evaluate their organizational maturity for all software implementations, including Excel, QuickBooks, and Microsoft Great Plains Dynamics. The assessments should be based on the premises that:

- All organizations are at risk due to a lack of resources or ineffective leadership, but SMEs are particularly at risk given the evidence from Sarbanes-Oxley implementations and research from the Association of Certified Fraud Examiners.
- A minimum of internal controls should be attained for any software implementation.
- Successful IT implementations are inextricably linked to qualified staff and effective project management. A priority for the audit committee, the board, corporate officers, and the external auditor is to understand the impact of IT requirements on internal controls, as IT domain weaknesses spill over to other IT and non-IT internal control effectiveness in other COSO domains.

Recruiting a qualified board for SMEs can be very challenging as qualified board members are in high demand and those who do qualify may want to avoid the board member liabilities associated with higher-risk SMEs. Recruiting qualified board and audit committee members for SMEs creates the potential for board members to add perspective, value, and oversight for financial reporting in a longer-term relationship. However, many prospective recruits to the board or audit committee may perceive excessive risk in a smaller company given the potential for shareholder litigation for a variety of reasons, including fraudulent financial reporting. Meaningful internal controls can facilitate board member recruiting.

Internal controls can be strengthened by active and visible participation by management in the internal controls for SMEs. For example, managers can review system reports of detailed transactions; select transactions for review of supporting documents;

oversee periodic counts of physical inventory, sign off on system access or program changes, and compare equipment or other assets with accounting records; and review reconciliations of account balances or perform them independently. In many SMEs, managers already are performing internal control procedures, but documentation is less than complete. Credit should be taken for their contribution to effective internal control through written job descriptions and logs that document the periodic steps taken to support their written job descriptions.

The authors believe that a critical success factor lies in an organization's capability to implement and maintain financial software while sustaining or improving internal controls. Most SMEs have the advantage of simpler operating requirements, which should translate into the acquisition of software packages to meet operating requirements and avoid risks associated with in-house developed systems. Maintenance and development are borne by the vendor, which is a much better choice than the IT staff of an SME who typically lack technical expertise in that particular software. Commercially available software can offer features for controlling data access, performing checks on data processing completeness and accuracy, completing system and data backup, and maintaining related documentation. Over the last decade, additional application controls have been added in Excel, QuickBooks, and Microsoft Dynamics as those products have evolved. Although management may be able to take the leadership in training operating staff on general and application controls, it is more likely that outside resources such as CPAs with sufficient depth in internal controls would be required for periodic consulting engagements. With appropriate training, application controls can help improve operational consistency, facilitate log reviews, automate reconciliations, provide meaningful exception reporting, and support proper segregation of duties.

RESEARCH CONFIRMING THE RISKS ASSOCIATED WITH SMEs

The awareness of control challenges associated with SMEs has increased significantly since the first pronouncement by the Committee of Sponsoring Organizations of the Treadway Commission (CSOTC) in 1992. It's reasonable to assume that controls that we associate with CSOTC were rarely in place for many SMEs up to and including the implementation of SOx. The events that followed the implementation SOx in 2002 include independent research from academia, congressional hearings, reports from the General Accounting Office (GAO), and eventually a new pronouncement by COSO in 2006 that shed light on the state of controls in SMEs. The report from the ACFE, *The 2012 Report to the Nation on Occupational Fraud and Abuse* (ACFE 2012), confirmed the vulnerability of businesses with fewer than 100 employees to fraud and higher average losses.

The original 1992 CSOTC report defined *internal control* as a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws

and regulations. Five concepts were emphasized by the 1992 CSOTC: (1) a sound control environment defined by a qualified board, the tone at the top, and competent personnel throughout the organizational structure; (2) ongoing risk assessment of financial reporting including the potential of fraud; (3) both procedural and information technology controls that respond to a broader risk assessment of the enterprise and the environment; (4) effective financial and internal control reporting; and (5) ongoing evaluations of the internal control environment to enable management to respond. COSO remains tethered to *Enterprise Risk Management—Integrated Framework* (ERM) whether it's an SME or a large public company. Following the 1992 pronouncement by CSOTC, numerous events, including the failure of Enron, the initial implementation of SOx in 2004, and subsequent assessments by the GAO, Congress, and COSO (2007), led to a reemphasis on the five components of COSO for SMEs whether they are public or private.

Independent research on firms that reported at least one material weakness for those companies in the initial SOx implementations from 2002 to 2005 found that these firms were more likely smaller, younger, riskier, more complex, and financially weaker, with poorer accrual earnings quality. In their independent research, Klamm and Watson (2009) examined 490 firms reporting material weakness in the first year of SOx compliance to evaluate the interrelatedness of weak COSO components and IT controls. Their research identified relationships between the reported material weakness and the five components of COSO, including:

- A weak control environment has a positive association with the remaining four weak COSO components; that is, COSO components are likely to affect one another.
- IT-related weak COSO components frequently spill over to create more non-IT-related material weakness and misstatements.
- IT-related weak COSO components negatively affect reporting reliability and add to the number of non-IT material weaknesses reported.

Moreover, the conclusion from Klamm and Watson's research is that the IT domain appears to affect overall control effectiveness.

Cumulative evidence from IT projects in the past 15 years and SOx suggest several risk drivers for internal controls, including:

- Complexity of the enterprise, including the number of subsidiaries and the nature of assets and liabilities
- Smaller, younger, riskier, more complex, and financially weaker organizations that lack either adequate resources or the leadership to execute an effective or controlled change management

The General Accounting Office (GAO 2006) in its *Report to the Committee on Small Business and Entrepreneurship*, U.S. Senate, in 2006, identified the resource limitations that make it more difficult for smaller public companies to achieve economies of scale, segregate duties and responsibilities, and hire qualified accounting personnel

to prepare and report financial information. Segregation of transactions and the associated division of responsibilities in a smaller company absorb a larger percentage of the company's revenues or assets than in a larger company. About 60 percent of the smaller public companies that responded to the GAO survey reported that it was difficult to implement effective segregation of duties. Several executives reported difficulty in segregating duties due to limited resources. Other executives in the GAO survey commented that it was difficult to achieve effective internal control over financial reporting because they lacked expertise within their internal accounting staff to complete the accounting for such complex topics as stock option valuations. So while it's more difficult to implement internal controls, the AICPA noted that smaller public companies often do not have the internal audit functions referred to in COSO's internal framework guidance and therefore cannot provide oversight (GAO 2006). The nature of SMEs creates difficulties with internal controls and oversight, leading to modified expectations for shareholder protection.

In connection with SOx compliance, the SEC requires the implementation of *Enterprise Risk Management—Integrated Framework* (ERM), authored by the Treadway Commission's Committee of Sponsoring Organizations (COSO 1992). The report, *Internal Control for Financial Reporting: Guidance for Smaller Public Companies*, issued in 2007 by COSO following the GAO report, reemphasizes the five concepts originally identified in 1992. The five concepts are:

1. A sound control environment defined by a qualified board, the tone at the top, and competent personnel throughout the organizational structure.
2. Ongoing risk assessment of financial reporting, including the potential of fraud.
3. Both procedural and information technology controls that respond to the risk environment.
4. Effective financial and internal control reporting.
5. Ongoing evaluations of the internal control environment to enable management to respond. COSO remains tethered to *Enterprise Risk Management—Integrated Framework* (ERM), whether it's an SME or a Fortune 100 enterprise, after the original pronouncement 14 years earlier.

In the *Internal Control for Financial Reporting: Guidance for Smaller Public Companies*, COSO reemphasized the need for management to weigh costs against benefits particularly for those companies that have focused considerable attention on the costs associated with Section 404 compliance. While the costs of internal control are apparent, the benefits of capital market access to provide funds for innovation and market expansion may not be as obvious. Additional benefits include more reliable financial reporting; consistent mechanisms for processing transactions across an organization; enhancing speed and reliability; and the ability to accurately communicate business performance to partners and customers. Private companies that do not rely on public financing still require bank financing and, potentially, external investors from time to time.

A FRAMEWORK FOR EVALUATING RISKS AND CONTROLS, COMPENSATORY CONTROLS, AND REPORTING DEFICIENCIES

A review of the Apple 1 business identified numerous internal control challenges that are associated with small businesses. Small staffs with the inability to segregate the transaction cycle, the potential for management override because of management's dominance of day-to-day activities, qualified accounting personnel with adequate training in Excel, QuickBooks, or Microsoft Dynamics, and maintaining current updates for software applications are among the control challenges for SMEs. All of these examples deliver threats to the ability of the enterprise to provide reliable financial transactions, accounting records, and financial statements. So when does a threat become a *material weakness* and which framework is applicable to making an assessment about the appropriateness of various controls?

In 2007, in the context of a Section 404 discussion within SOx (SEC 2007a), the SEC delivered clarification on the term *material weakness* as "a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis." A *significant deficiency* exists if one or more control deficiencies exist that create a financial reporting misstatement that rises to a level that is less than a material weakness. "Our guidance enables companies of all sizes to focus on what truly matters to the integrity of the financial statements—risk and materiality," said Securities and Exchange Commission chief accountant Conrad Hewitt. While the following discussion applies to publicly traded SMEs, the principles provide a framework for risks and controls for financial reporting for all SMEs irrespective of the capital structure and the ultimate regulatory framework.

The SEC delivered its interpretative guidance in 2007 for public companies of all sizes, including publicly listed SMEs, around two key principles:

1. Management should evaluate whether it has implemented controls that adequately address the risk that a material misstatement of the financial statements would not be prevented or detected in a timely manner using a top-down, risk-based approach including the role of entity-level controls (including general controls).
2. The evaluation procedures should be aligned with those areas of financial reporting that pose the highest risks to reliable financial reporting with more extensive testing in high-risk areas.

For principle 2, the evaluation procedures include a five-step process that requires management:

1. To identify those risks of misstatement that could, individually or in combination with others, result in a material misstatement of the financial statements
2. To evaluate whether it has controls placed in operation to adequately address the company's financial reporting risks

3. To consider the nature of the entity-level controls and how those controls relate to the financial reporting element
4. To consider the adequacy of both general controls and application controls for IT processing underlying the integrity of financial statement reporting
5. To maintain reasonable support for its assessment, including documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks

Management should be able to assess the financial reporting risks underlying their internal controls. (See Figure 1.2.) Higher risks associated with financial reporting risks require more evidence; lower risks associated with financial reporting require less evidence.

In the SEC's interpretive guidance in 2007 of how to assess Section 404 of SOx, an example of how management should evaluate the likelihood of the possibility of a control failure included an assessment of eight attributes of controls, all of which are applicable to SMEs (SEC 2007b). Management's assessment of financial reporting misstatements includes both the materiality of the financial reporting element and the susceptibility of the underlying account balances, transactions, or other supporting information to a misstatement that could be material to the financial statements. The attributes that would be evaluated are:

1. The type of control (i.e., manual or automated) and the frequency with which it operates
2. The complexity of the control
3. The risk of management override

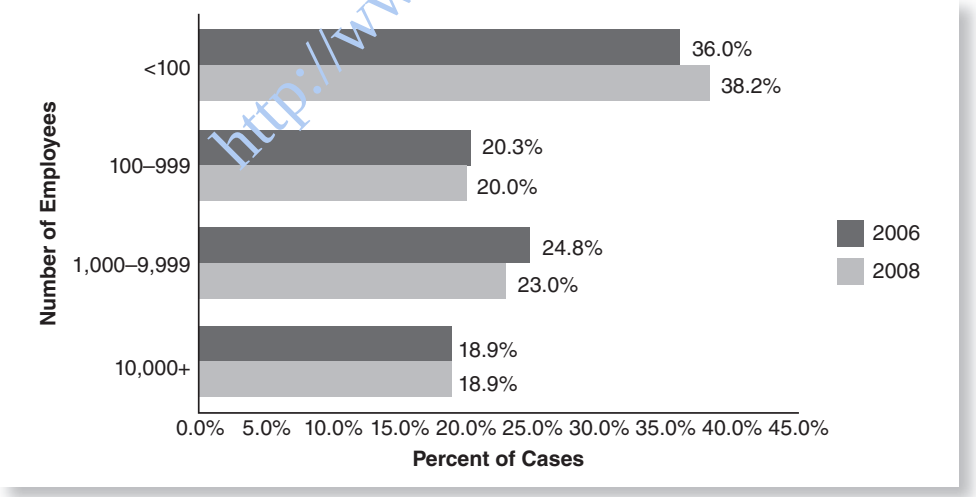

FIGURE 1.2 Determining the Sufficiency of Evidence Based on Internal Control over Financial Reporting (ICFR) Risk

Source: Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934 (SEC 2007b), www.sec.gov/rules/interp/2007/33-8810.pdf.

4. The judgment required to operate the control
5. The competence of the personnel who perform the control or monitor its performance
6. Whether there have been changes in key personnel who either perform the control or monitor its performance
7. The nature and materiality of misstatements that the control is intended to prevent or detect
8. The degree to which the control relies on the effectiveness of other controls (e.g., IT general controls), and evidence of the operation of the control from prior year(s)

Evaluation of these eight attributes could be applied to the Apple 1 business described earlier and to any SME that employed Excel, QuickBooks, or Microsoft Dynamics.

A *risk-based audit approach* (Romney and Steinbart 2011):

1. Determines the threats.
2. Identifies the control procedures to prevent, detect, or correct the threats.
3. Evaluates that the controls that are purported to exist actually exist.
4. Makes a final determination as to whether the purported controls are adequate or effective and whether additional audit procedures should occur.

After determining the threats in Step 1, Step 2 in the risk-based audit approach, the identification phase, includes all controls that management has put into place. Step 3, the evaluation step, includes a system review to determine whether control procedures are in place and tests to determine whether the controls are working as intended. If the controls are inadequate or ineffective in Step 4, compensating controls should be considered as a replacement for the primary controls. The SEC defines *compensating controls* as controls that serve to accomplish the objective of another control that did not function properly, helping to reduce risk to an acceptable level. To have a mitigating effect, the compensating control should replace the original control to prevent or detect a material misstatement to the financial statements.

A sample framework for the audit of QuickBooks processing controls integrating a risk-based audit approach would include the following assessment in four categories.

Types of Errors and Fraud

The types of errors and fraud determinants in the framework include:

- Failure to detect incorrect, incomplete, or unauthorized input data (e.g., override by management)
- Failure to properly correct errors flagged by data editing procedures
- Introduction of errors into files or databases during updating (e.g., updates from add-in inventory system that were not reviewed using reasonableness tests, or management override)
- Improper distribution or disclosure of QuickBooks output (e.g., password controls with strong passwords)

- Intentional or unintentional inaccuracies in reporting (e.g., a monthly review of reports on missing inventory, excessive credit memos, or adjustments to accounts receivable)

Control Procedures

The control procedures in the framework include:

- Data editing routines of source data
- Reconciliation of batch totals
- Effective error correction procedures (e.g., management approval for voiding or deleting transactions in QuickBooks)
- Competent supervision of QuickBooks with trained personnel
- Effective handling of data input and output by data control personnel (e.g., predefined user roles are available in the Enterprise edition of QuickBooks, which limit a user's role in extreme detail)
- Maintenance of proper environmental conditions in the computer facility (e.g., locked server cabinets, background checks on key personnel, etc.)

Audit Procedures

The audit procedures in the framework that follow fall into two categories: system review and tests of controls.

System Review

- Review administrative documentation for processing control standards (e.g., a review of the logs of management approval for voided or deleted transactions).
- Review systems documentation for data editing and other processing controls (e.g., a review of logs of data backup and testing of files).
- Document operations for completeness and clarity.
- Observe computer operations and data control functions.

Tests of Controls

- Evaluate adequacy of processing control standards and procedures.
- Evaluate adequacy and completeness of data editing controls.
- Verify adherence to processing control procedures by observing computer and data.
- Verify that application system output is properly distributed.
- Reconcile a sample of batch totals; follow up on discrepancies.
- Trace a sample of data edit routines errors to ensure proper handling.
- Verify processing accuracy of sensitive transactions (e.g., management approval for accounts receivable write-offs).
- Verify processing accuracy of computer-generated transactions (e.g., test credit card transactions).
- Check accuracy and completeness of processing controls by using test data (e.g., the transaction list by vendor should be reviewed for check detail, purchases by vendor detail, purchases by item detail, open purchase orders, and budget vs. actual).

Compensating Controls

Finally, the Audit Trail Report in QuickBooks is an example of a compensating control to use to answer three essential questions:

1. Who added/edited/deleted the transaction?
2. When was the transaction added/edited/deleted?
3. What were the relevant details of the transaction (i.e., date, amount, accounts, names)?

SUMMARY: THE ROAD AHEAD

A robust implementation of COSO's *Internal Control—Integrated Framework*, and an implementation of the Control Objectives for Information and related Technology (COBIT) framework, are effective responses to the risk drivers for the SME. The authors believe that the board, management, IT, business operations, and accounting organization must be able to support COSO on a *systematic and repeatable level*—and that the controls are integral to the operation of the enterprise. The authors also believe that even with commercially available financial applications, organizational maturity may be a major risk factor for SMEs as evidenced by the conclusions of reports of SOx compliance, GAO, ACFE, the U.S. Secret Service, Verizon, and others. Given the high level of risk exposure to fraud and abuse in SMEs and low levels of success attributable to external audit and the near-absence of internal audits in small businesses, effective internal controls and COSO compliance are critical success factors in the financial health of the SME.