Chapter 1

The SOX Saga

In This Chapter

- Riding the wave of political support for SOX
- Looking at the loopholes SOX closed
- Surveying SOX's impact
- Debunking some common media myths about SOX

In response to a loss of confidence among American investors reminiscent of the Great Depression, President George W. Bush signed the Sarbanes-Oxley Act into law on July 30, 2002. SOX, as the law was quickly dubbed, is intended to ensure the reliability of publicly reported financial information and bolster confidence in U.S. capital markets. SOX contains expansive duties and penalties for corporate boards, executives, directors, auditors, attorneys, and securities analysts.

Although most of SOX's provisions are mandatory only for public companies that file a Form 10-K with the Securities and Exchange Commission (SEC), many private and nonprofit companies are facing market pressures to conform to the SOX standards. Privately held companies that fail to reasonably adopt SOX-type governance and internal control structures may face increased difficulty in raising capital, higher insurance premiums, greater civil liability, and a loss of status among potential customers, investors, and donors.

In this chapter, I take a look at the political impetus for SOX and summarize some key provisions of the SOX statute in plain English. I also dispel a few common SOX myths.

The Politics of SOX

SOX passed through both houses of Congress on a wave of bipartisan political support not unlike that which accompanied the passage of the U.S. Patriot Act after the terrorist attacks of 2001. Public shock greased the wheels of the political process. Congress needed to respond decisively to the Enron media fallout, a lagging stock market, and looming reelections (see Chapter 2 for

details). SOX passed in the Senate 99–0 and cleared the House with only three dissenting votes.

Because political support for SOX was overwhelming, the legislation was not thoroughly debated. Thus, many SOX provisions weren't painstakingly vetted and have since been questioned, delayed, or slated for modification.

For the past 70 years, U.S. securities laws have required regular reporting of results of a company's financial status and operations. SOX now focuses on the accuracy of what's reported and the reliability of the information-gathering processes. After SOX, companies must implement internal controls and processes that ensure the accuracy of reported results.

Prior to SOX, the Securities Act of 1933 was the dominant regulatory mechanism. The 1933 Act requires that investors receive relevant financial information on securities being offered for public sale, and it prohibits deceit, misrepresentations, and other fraud in the sale of securities.

The SEC enforces the 1933 Act requiring corporations to register stock and securities they offer to the public. The registration forms contain financial statements and other disclosures to enable investors to make informed judgments in purchasing securities. (For more about the securities registration process, flip to Chapter 3.) The SEC requires that the information companies provide be accurate and certified by independent accountants.

SEC registration statements and prospectuses become public shortly after they're filed with the SEC. Statements filed by U.S. domestic companies are available on the EDGAR database accessible at `www.sec.gov`.

A loophole under prior law

SOX provides that publicly traded corporations of all sizes must meet its requirements. However, not all securities offerings must be registered with the SEC. Some exemptions from the registration requirement include:

- Private offerings to a limited number of persons or institutions
- Offerings of limited size
- Intrastate offerings
- Securities of municipal, state, and federal governments

The SEC exempts these small offerings to help smaller companies acquire capital more easily by lowering the cost of offering securities to the public.

In contrast, SOX provides that publicly traded corporations of all sizes must meet certain specific requirements depending on the size of the corporation.

Not everyone's a SOX fan

Only three Congressmen opposed the 2002 passage of SOX: GOP Representatives Ron Paul of Texas, Jeff Flake of Arizona, and Mac Collins of Georgia. Congressman Flake observed:

> *Obviously there are businesses that were acting in a fraudulent manner. We still have that today, and there are laws on the books that thankfully are being used more aggressively today to get at these businesses. But when we react so quickly, sometimes without the best knowledge of how to do this, without some of these investigations taking their course, without these enforcement agencies giving us full recommendations, then we have unintended consequences.*

In the years after SOX, many businesses and politicians are echoing the sentiments of Congressman Flake. The greatest criticism has been the financial burden imposed on small companies. The SEC received so many complaints about the disproportionately high costs of compliance for smaller public companies that it convened an Advisory Committee on Smaller Public Companies to investigate them. In response, the SEC has voted twice to extend the compliance deadline for Section 404 smaller public companies, called *non-accelerated filers,* primarily because it has acknowledged that the costs of compliance for smaller companies greatly exceeded estimates. (Section 404 is discussed in Chapter 11.)

The SEC extended the deadline for small-cap companies by one year, voting in March 2005 to push the compliance date to July 2006. When this extension failed to stop the grumbling about costs and confusion about compliance, the SEC decided in September 2005 that small companies wouldn't be required to comply with the Section 404 requirements until their first fiscal year ending on or after July 15, 2007.

In addition to the burden on small business, SOX is criticized for the sheer confusion it has created. SOX requires accounting firms and companies to simultaneously monitor several evolving sets of interpretive standards from the SEC and the Public Company Accounting Oversight Board (PCAOB). Early attempts to implement SOX have been accompanied by more resignations within regulatory agencies than shake-ups in corporate boardrooms. (The PCOAB is on its third chairman in as many years, as discussed in Chapter 6, and turnover at the SEC has been equally eventful since SOX.) most studies have shown that SOX has impacted the composition and behavior of corporate boards, to date, less than expected.

Regulatory confusion isn't the only culprit; many companies have contributed to their own SOX woes by simply failing to plan properly. The start-up costs of any initiative are always highest in the beginning; however, many companies simply panicked, hiring teams of expensive consultants and launching overlapping and ill-conceived projects to document their controls under SOX. This initial "spare-no-expense" approach may have helped some companies meet a deadline, but it also established the framework for new internal bureaucracy.

A final, broader criticism waged against SOX is its effect on the competitiveness of U.S. businesses. Many argue that SOX is a major distraction from the core activities of businesses, making them less viable in a global marketplace. Management must spend more time jumping through regulatory hoops and less time innovating. Arguably, SOX also makes it more difficult and costly for technologically innovative companies to raise capital by selling their stock on U.S. exchanges because of the increased regulatory burden. (See Chapter 3 for an explanation of securities registration requirements and stock exchanges.)

New ammunition for aggrieved investors

SOX now gives public companies specific directives as to how financial information offered to the public must be compiled, yet, as Chapter 16 discusses, it stops short of giving investors a right to sue companies privately for failing to meet these standards. Rather, with the exception of SOX Section 306 (dealing with stock trading during pension fund blackout periods), investors must wait for the SEC and Justice Department to bring actions against companies for SOX violations. Investors can't hire their own lawyers to initiate action on their behalf.

Although there's no "private right" to sue directly under SOX, shareholders and litigants are in a much stronger position after SOX than under the old federal and state statutes. Prior to SOX, federal and state laws didn't establish specific standards for corporations in *compiling* the information they fed to the public in their financial reports. In the event that investors were damaged or defrauded, the investors themselves were responsible for persuading judges the information they had received wasn't truthful or accurate, without reference to any specific standards. Aggrieved investors had only an amorphous body of analogous facts from prior court cases to try to convince courts to apply their specific situation. Now plaintiffs may strengthen their claims and arguments by referencing the standards set forth in SOX.

Corporate America after SOX

SOX goes where the federal government has never gone before. Although federal regulation of the sale of securities to protect the public is nothing new, SOX goes beyond simply prohibiting deceptive conduct and misrepresentations — it actually tells public corporations how they must run themselves, and creates a new environment for nonpublic companies and nonprofits.

SOX defines specific duties for employees and board members and dictates the structure of boards of directors. It even tells corporations how they have to conduct their day-to-day operations to prevent theft and misappropriation, requiring them to maintain adequate internal controls. (I talk more about internal controls in Chapter 11.) SOX also elbows out state governments in their traditional roles of governing corporations, making corporate law in the United States much more federalized.

Who Combats Corruption under SOX?

SOX is a multidisciplinary piece of legislation that regulates several professions simultaneously. Board members, auditors, attorneys, management, small business owners, and even rank-and-file employees all have their own statutorily scripted roles to play.

The independent audit board

One of the most significant reforms introduced by SOX is the advent of the independent audit board. SOX requires corporations to have audit committees made up solely of *independent* directors. Board members are considered independent in the sense that they receive no salary or fees from the company other than for services as directors.

The audit committee is responsible for obtaining information from management relevant to the audit and otherwise assisting in the audit process. It's viewed as an important part of a company's internal control because it provides a company presence entirely independent from management and interfaces with the independent auditors (from an outside firm). For more coverage of the audit committee's responsibilities, check out Chapter 7.

Ironically, one firm that would have been able to comply with the SOX director independence requirements *before* the law was passed was Enron. Eighty-six percent of Enron's board was independent. A former dean of the Stanford Business School and professor of accounting chaired its audit committee. Yet when the scandal broke, the professor claimed he didn't understand the audit documentation.

SOX presumes that boards made up of independent directors will look out for shareholders' interests and ask auditors to more carefully review management policies and decisions that can affect profitability. However, in the end, an independent audit committee isn't a panacea and doesn't guarantee objectivity in the audit process. The committee, the board, and the auditors all must rely on the accuracy of the information they get from management and on management to recognize, anticipate, and prevent problems.

SOX regulates the membership composition of boards but doesn't specifically regulate their behavior.

Evolving auditors

Auditors are the traditional arbiters of accurate information within a company. They're the accountants responsible for testing the accounting data gathered from management and from rank-and-file employees. Auditors may be either internal employees of a company or independent auditors working for an outside firm.

Both internal and independent auditors adhere to Generally Accepted Accounting Principles (GAAP). GAAP is a term that refers to the rules established by the Financial Accounting Standards Board, the American Institute of Certified Public Accountants, and the SEC, which is the standard-setting body for publicly traded U.S. companies and the exchanges that list their stock.

GAAP contains a number of provisions designed to ensure auditors' independence, objectivity, and professionalism. An auditor must certify that a company's financial statements are fairly presented in accordance with GAAP and contain no material irregularities that would adversely affect reported results.

Traditionally, auditors have been viewed as pretty trustworthy people. The Enron scandal that led to the demise of the nation's largest independent auditing firm, Arthur Andersen, changed all that. Congress and the public were shocked that one of the world's largest corporations (Enron) could collapse within five months of receiving a clean opinion from its auditors (Andersen). (I talk more about the Enron and Arthur Andersen stories in Chapters 2 and 5.)

At the Enron trials, senior managers testified that the auditors never brought material issues to the managers' attention. The managers claimed that although they had ultimate responsibility for what was included in the financial statements with the SEC, they couldn't know what the auditors didn't tell them or failed to bring to their attention. It also came to light that the so-called independent auditors weren't so independent. In addition to providing audit services, they provided a myriad of highly lucrative consulting, tax, and other support services to Enron, which meant that the audit firm had tremendous financial incentives to stay on good terms with Enron, rather than being vocal about the company's accounting flaws.

Enron wasn't the only scandal that tainted the audit industry. During the Savings and Loan (S&L) crisis of the 1980s, auditors failed to take into account the industry's shift from home loans to riskier real estate ventures and junk bonds. As a result, many S&Ls went bankrupt just months or even weeks after getting clean opinions from their auditors.

To resolve problems associated with self-regulation (which had previously been the norm for the accounting profession), SOX creates the Public Company Accounting Oversight Board (PCAOB), a regulatory oversight board. This board is charged with the enormous responsibilities of setting ethics and conflict of interest standards as well as disciplining accountants and conducting annual reviews of large accounting firms. (For more on the PCAOB, turn to Chapter 6.)

Not only has the accounting profession suffered the loss of the right to regulate itself, but it can no longer market and compete for business in the same way. SOX makes it unlawful for a registered audit firm to provide many types of nonaudit services to its clients that were formally its bread-and-butter. For example, an audit firm can't provide bookkeeping, financial information systems design, appraisal, evaluation, actuarial, or investment services to clients it audits. (However, audit firms can make up some, if not all, of this lost income by performing internal control audits under Section 404 of SOX; see Chapter 12.)

According to a survey of 32 mid-sized companies by the law firm Foley & Lardner, accounting, audit, and legal fees also doubled under Sarbanes-Oxley. The costs of directors' liability insurance skyrocketed from $329,000 to $639,000.

Lawyers' noisy new liability

Incident to its authority to make rules under SOX, the SEC has proposed a controversial *noisy withdrawal* rule for attorneys. The rule would require a lawyer who learns of a corporate client's wrongdoing to alert SEC regulators to the nature of any ongoing fraud before withdrawing from representation. Attorneys who are unable to persuade a corporate client to mend its ways would be required to notify the SEC that they are withdrawing from representation. Not surprisingly, opponents have argued that the rule violates traditional concepts of attorney-client privilege. However, the American Bar Association has taken the position that noisy withdrawal doesn't violate the privilege.

CEOs and CFOs

SOX forces chief executive officers (CEOs) and chief financial officers (CFOs) of corporations to take responsibility and possibly face criminal penalties for earnings misstatements. They're required to certify in writing that the information appearing in the company's report is a fair and accurate representation of the company's financial status and activity.

Not only do criminal penalties apply if officers and directors misstate financial information, but these individuals also can be required to give back their bonuses to compensate the company for the costs of redoing the financial statements. (For more on the consequences officers and directors face for misstatements, check out Chapter 2.) Under SOX, each member of management is expected to certify that he or she runs a clean ship — no excuses.

Small businesses and nonprofits in the headlights

Although SOX was passed to deal with mega-scandals like Enron and WorldCom, it's becoming a catastrophe for American small business. As of this writing, although the wording of the SOX statute technically applies only to publicly traded corporations, it's the benchmark against which every privately held company's financial and corporate governance practices are measured.

Banks and insurance companies report that they now ask small, privately held companies about their internal controls and audit procedures. Failure to answer convincingly can result in more costly credit or higher insurance premiums.

Nonprofits, which can't afford a hint of scandal that may ruin their credibility with donors, are rushing to adopt governance and conflict-of-interest policies in line with SOX.

Start-ups and new ventures are facing increased hurdles as they attempt to "go public" by becoming eligible to list their stock on exchanges.

The rank-and-file

SOX imposes new burdens on rank-and-file employees, often requiring them to adhere more carefully to company procedures or to complete additional documentation to carry out new internal control measures. However, SOX empowers blue-collar and other nonmanagerial employees in other ways:

- Section 301(4) requires publicly traded companies to collect, retain, and resolve complaints from employees.
- Section 806 specifically protects whistle-blowers who report violations of law or company policy from suffering retaliation by the company.

New high–paid governance gurus

Nearly every public company has designated specific management or legal personnel responsible for overseeing corporate governance policies. A 2005 survey posted on Salary.com reported compensation for many top global ethics and compliance executives to be approaching $750,000.

A Summary of SOX: Taking It One Title at a Time

The SOX statute is more or less an outline, with full details coming in the form of Securities Exchange Commission (SEC) rules for implementation as well as pronouncements from the newly created Public Company Accounting Oversight Board (PCAOB). Most of SOX's provisions currently apply to public companies that file Form 10-K with the SEC; however, more and more companies are opting for voluntary compliance to insulate themselves from future litigation risks and unforeseen management liabilities.

This section is intended to give you a broad view of what the new law contains and what it requires of today's companies in the United States.

Title I: Aiming at the audit profession

At its outset, SOX establishes a five-member Public Company Accounting Oversight Board (PCAOB) that lets auditors know what they're supposed to be evaluating and sets rules about the relationships and ties auditors can have with the companies they audit. Title I provides for change in six major areas:

- **The PCAOB:** The SEC oversees the PCAOB, which is funded through fees collected from issuers. The PCAOB (affectionately nicknamed "Peek-a-boo" by many auditors, attorneys, and other professionals) has the following responsibilities:
  - **To oversee the audit of public companies:** The accounting profession used to regulate itself through a voluntary organization known as the American Institute of Certified Public Accountants (AICPA), but Enron proved that the old system didn't work very well.
  - **To establish audit report standards and rules:** Auditors wait avidly for the issue of these standards and rules to clear up confusion and aid them in performing their day-to-day duties after SOX.
  - **To register audit firms:** The PCAOB is in charge of registering, inspecting, investigating, and enforcing compliance of public accounting firms as well as CPAs and other people in the profession. Any public accounting firm that participates in any audit for a company covered by SOX is required to register with the PCAOB.

  Critics have noted the Public Company Accounting Oversight Board would have been more appropriately named the Public Company *Auditing* Oversight Board.

- **Work paper retention:** Title I contains some new administrative requirements for auditors, including a rule that audit firms retain all their work papers for seven years.
- **Two-partner requirement:** Two partners now have to sign off on every audit, as discussed further in Chapter 5.
- **Evaluation of internal control:** Auditors must evaluate whether the companies they audit have internal control structures and procedures that ensure that their financial records accurately reflect transactions and disposition of assets. Auditors must also assess whether the companies appropriately authorize receipts and expenditures and verify that transactions are made only with authorization of senior management. If companies don't have adequate internal controls in place, the auditors must describe any material weaknesses in the internal control structures and document instances of material noncompliance.

- **Inspections of audit firms:** Auditors must submit to continuing inspections by the PCAOB. Firms that provide audit reports for more than 100 public companies get inspected once a year. Firms that audit fewer than 100 companies get reviewed every three years.

Title I of SOX also empowers the PCAOB to impose disciplinary or remedial sanctions upon audit firms.

Title II: Ensuring auditor independence

Title II of SOX focuses on conflicts of interests arising from close relationships between audit firms and the companies they audit; namely, it prohibits auditors from performing certain nonaudit services to clients they audit. However, SOX allows *audit committees* (internal committees charged with overseeing the audit process within publicly traded companies) to approve some activities for nonaudit services that aren't expressly forbidden by Title II of SOX (see Chapter 7 for more on audit committees and nonaudit services).

To further protect against conflicts of interest, audit partners must be rotated to prevent individuals from getting too close to the companies they audit. Specifically, a partner is prevented from being the lead or reviewing auditor for more then five consecutive years. Also, an auditor faces a one-year prohibition if the company's senior executives were employed by that audit firm during the one-year period preceding the audit initiation date. Title II also requires auditors to report to the audit committee on accounting policies used in the audit and document communications with management.

Title III: Requiring corporate accountability

This section of SOX focuses on the company's responsibility to ensure that the financial statements it distributes to the public are correct. Its two main provisions include:

- **Establishment of audit committees:** SOX requires each company subject to SOX to form a special audit committee. Each member of the audit committee must be a member of the board of directors but otherwise *independent* in the sense that he or she receives no other salary or fees from the company.
- **Management certification:** Title III requires CEOs and CFOs to certify:
  - That periodic financial reports filed with the SEC don't contain untrue statements or material omissions
  - That financial statements fairly present, in all material respects, the financial conditions and results of operations

- The company's chief executive and chief financial officers are responsible for internal controls, and that the internal controls are designed to ensure that management receives material information regarding the company and any consolidated subsidiaries
- That internal controls have been reviewed within 90 days prior to the report
- Whether there have been any significant changes to the internal controls

Title III also makes it unlawful for corporate personnel to exert improper influence upon an audit for the purpose of rendering financial statements materially misleading.

- **Bonuses:** Title III requires a company's CEO and CFO to forfeit certain bonuses and compensation received if the company has to issue corrected financial statements (called *restatements*) due to noncompliance with SEC rules.
- **Bans on stock trades during blackout periods:** Title III bans directors and executive officers from trading their public company's stock during pension fund blackout periods. It also obligates attorneys appearing before the SEC to report violations of securities laws and breaches of fiduciary duty by a public company. For the benefit of victims of securities violations, Title III creates a special disgorgement fund that's funded by the fines companies have to pay to the SEC.

Title IV: Establishing financial disclosures, loans, and ethics codes

This section contains several key SOX provisions, including:

- **Disclosure of adjustments and off–balance sheet transactions:** Financial reports filed with the SEC must reflect all material corrections to the financial statements made in the course of an audit. Title IV also requires disclosure of all material off–balance sheet transactions and relationships that may have a material effect upon the financial status of an issue.
- **Prohibition of personal loans extended by a corporation to its executives:** Such loans are prohibited if they're subject to the insider lending restrictions of the Federal Reserve Act.
- **Disclosure of changes to inside stock ownership:** Senior management, directors, and principal stockholders have to disclose changes in their ownership of corporate stock within two business days of making the transaction.

- **Internal control certification:** The now-famous Section 404 provides that annual reports filed with the SEC must include an internal control report stating that management is responsible for the internal control structure and procedures for financial reporting. The report should also state that management assesses the effectiveness of the internal controls for the previous fiscal year.
- **Code of ethics:** Companies subject to SOX must disclose whether they have adopted a code of ethics for their senior financial officers and whether their audit committees have at least one member who is a financial expert. (For more on the financial expert requirement, flip to Chapter 7.)
- **Regular SEC review:** Article IV requires regular SEC reviews of the disclosure documents companies file each year with the SEC.

Title V: Protecting analyst integrity

This section of SOX is aimed at preventing several types of conflicts of interest; among other things, it restricts the ability of investment bankers to preapprove research reports and ensures that research analysts aren't supervised by persons involved in investment banking activities. Title V prohibits employer retaliation against analysts who write negative reports, and it requires specific conflict of interest disclosures by research analysts who make information available to the public.

Title VI: Doling out more money and authority

This section authorizes the SEC to spend at least $98 million to hire at least 200 qualified professionals to oversee auditors and audit firms.

Title VI also gives the SEC the authority to

- Censure persons appearing or practicing before it for unethical or improper professional conduct. Title VI also directs federal courts to prohibit persons from participating in small (penny) stock offerings if the SEC initiates proceedings against them.
- Consider orders of state securities commissions when deciding whether to limit the activities, functions, or operations of brokers or dealers.

Title VII: Supporting studies and reports

This section of SOX funds and authorizes a number of reports and studies that, for example,

- Look at factors leading to the consolidation of public accounting firms and its impact on capital formation and securities markets.
- Address the role of credit-rating agencies in the securities markets.
- Examine whether investment banks and financial advisors assisted public companies in earnings manipulation and obfuscation of financial conditions.

Title VIII: Addressing criminal fraud and whistle-blower provisions

Title VIII imposes criminal penalties (maximum 10 years in prison) for knowingly destroying, altering, concealing, or falsifying records with intent to obstruct or influence a federal investigation or bankruptcy matter. It also imposes sanctions on auditors who fail to maintain for a five-year period all audit or review work papers pertaining to securities issuers. It makes certain debts incurred in violation of securities fraud laws nondischargeable in bankruptcy.

Title VIII also extends the statute of limitations for private individuals to sue for securities fraud violation. Individuals can sue no later than two years after the violation is discovered or five years after the date of the violation.

Finally, Title VIII provides whistle-blower protection by prohibiting a publicly traded company from retaliating against an employee who assists in a fraud investigation; executives who target whistle-blowers are subject to fines or imprisonment of up to 25 years. (For more on the whistle-blower provision, check out Chapter 16.)

Title IX: Setting penalties for white-collar crime

This section increases penalties for mail and wire fraud from 5 to 20 years in prison and penalties for violations of the Employee Retirement Income Security Act of 1974 to up to $500,000 and 10 years in prison.

In particular, Title IX establishes criminal liability for corporate officers who fail to certify financial reports, including maximum imprisonment of 10 years for knowing that the periodic report doesn't comply with SOX and 20 years imprisonment for willfully certifying a statement known to be noncompliant.

Title X: Signing corporate tax returns

This section of SOX expresses that a corporation's federal income tax return "should" be signed by its chief executive officer.

Title XI: Enforcing payment freezes, blacklists, and prison terms

Title XI adds to the criminal penalties aimed at fraud that are established by SOX's other sections. This section amends federal criminal law to establish a maximum 20-year prison term for tampering with a record or otherwise impeding an official proceeding. It also authorizes the SEC to seek a temporary injunction to freeze "extraordinary payments" to corporate management or employees under investigation for possible violations of securities law. Currently, there's no specific definition as to what constitutes an "extraordinary payment." However, Chapter 16 discusses some interesting litigation in this area (particularly the Gemstar case). This section also prohibits persons who violate state or federal laws governing manipulative, deceptive devices and fraudulent interstate transactions from serving as officers or directors of publicly traded corporations.

Finally, Title XI increases penalties for violations of the Securities Exchange Act of 1934 to up to $25 million dollars and up to 20 years in prison.

Some Things SOX Doesn't Say: SOX Myths

Although SOX costs corporations billions of dollars and diverts massive resources from production and profit-generating activities, it's not all bad. In fact, there are things it doesn't require; this section puts to rest four common SOX myths.

Myth #1: Auditors can't provide tax services

SOX doesn't segregate to absurd extremes the services accountants can provide to companies. For example, in passing SOX, Congress recognized that in many cases it's practical and cost-efficient for audit firms to prepare tax returns.

Although SOX precludes auditors from providing certain services to their clients to prevent Enron-type conflicts of interest, the legislation doesn't ban tax preparation services outright. Rather, the company's audit committee is charged with the responsibility of determining who provides tax services. However, some caveats must be considered in each case; for example, SOX's ban on software consulting may sound a death knell for audit firms that sell tax software to their audit clients and provide consulting services to support it.

Myth #2: Internal control means data security

Internal control refers to financial controls that impact financial statements, not data security. SOX doesn't specifically spell out any data security requirements for companies. Other legislation, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has rules about data security, but SOX is silent on things like password protection and encryption standards. This myth likely results (at least in part) from SOX's emphasis on internal control, which is a term sometimes used by information technology professionals.

Myth #3: The company isn't responsible for functions it outsources

Not true. Under SOX Section 404, it doesn't matter whether you outsource a system, process, or control or handle it internally — if it impacts the financial statements, the reporting company is on the line. This means you may have to directly test the controls at your outside service providers. Or, in some circumstances, you may be able to get a special type of report called an SAS 70 (type 2) from the service provider; this report documents the effectiveness of the provider's internal controls. (For more on the SAS 70 report, flip to Chapter 13.)

Myth #4: My company met the deadline for Section 404 first-year compliance. We're home free!

Sorry, 404 certification is an annual event. And when it comes to Section 404 compliance, a corporation is never "done." Compliance is a continual and ongoing process. Your systems must evolve as the company evolves, and so must the tests that are performed on those systems.