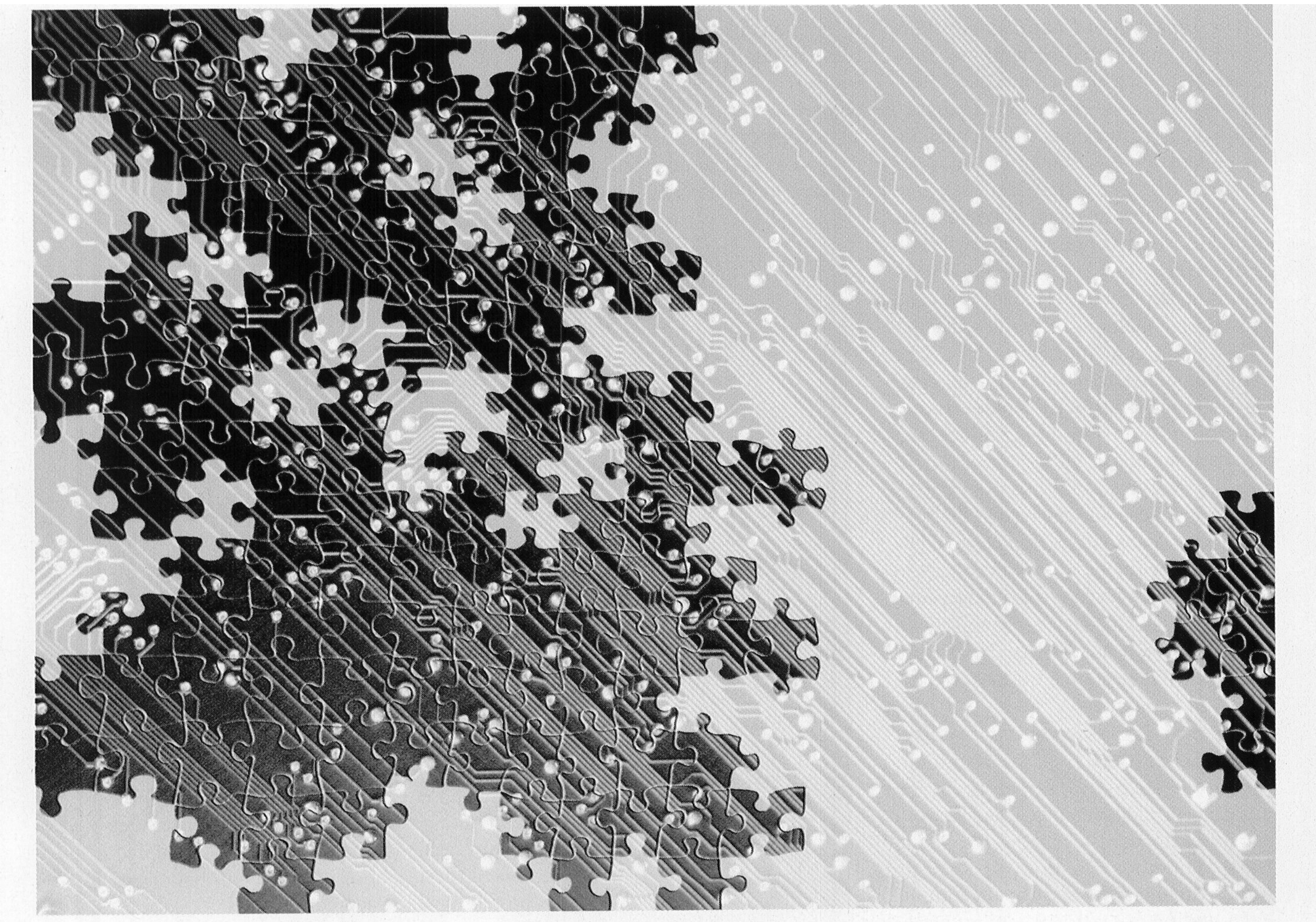


Sarbanes-Oxley Compliance for Nonaccelerated Filers

Solving the Internal Control Puzzle

By Sid M. Edelstein

No business legislation in recent history has elicited a broader range of reaction among financial professionals than the Sarbanes-Oxley Act of 2002 (SOA). While SOA clearly presents compliance challenges for public companies of all sizes, for many smaller, nonaccelerated filers these challenges can seem all but insurmountable. For some, this perception can lead to willful denial that compliance requirements extend to them. For others, it typically yields token efforts at compliance that often fall short. Neither is a good response. Unfortunately, many smaller companies lack the internal resources and specialized expertise necessary to successfully address all of the complexities associated with comprehensive SOA compliance.

Much of the standard professional auditing literature and available guidelines focuses almost exclusively on the objective analysis of accounting system control activities that support the financial reporting process. As a result, many auditors may find themselves ill equipped to address some of the more subjective and technically unfamiliar internal control aspects of SOA compliance audits: internal control framework development methodologies, the risk assessment activities on which they depend, and the information technology (IT) and business process automation systems that facilitate them.

Because business technology plays a major role in most companies' internal control activities, IT-related aspects of SOA compliance are not commonly addressed in typical accounting literature. Such IT aspects include the COBIT IT internal control and governance framework, as well as IT general controls than can potentially impact the accuracy and timeliness of a company's financial reporting processes. The historical development of COSO's *Internal Control–Integrated Framework* and an overview of its key elements form the conceptual underpinnings of corporate internal control systems.

A Short History of Decay

Sarbanes-Oxley is not the first time that government has tried to protect the public from corporate malfeasance. A similar spate of high-profile corporate scandals in the 1980s prompted the establishment of the Treadway Commission, which laid the foundation for a variety of meaningful accounting and financial reporting reforms. Today's SOA provisions are the direct descendants of these reforms. They are also only the first round in what is likely to become an ongoing legislative effort to improve corporate governance and accountability.

The Treadway Commission's charter recognized the need to improve corporate internal control over financial recordkeeping and accounting practices. The task of addressing this issue fell to a group of private organizations known as the Committee of Sponsoring Organizations (COSO). COSO's primary contribution to the Treadway Commission's efforts was the development of an open, integrated framework for analyzing and improving the effectiveness of internal controls. Officially published in 1992, COSO's *Internal Control–Integrated Framework* has become the de facto standard for internal control analysis and reporting. While leaving the door open to other potential internal control development frameworks, both the SEC and the PCAOB have specifically sanctioned the COSO framework as an appropriate guideline for SOA-compliant internal control analysis, development, and documentation.

Overview of the COSO Integrated Framework

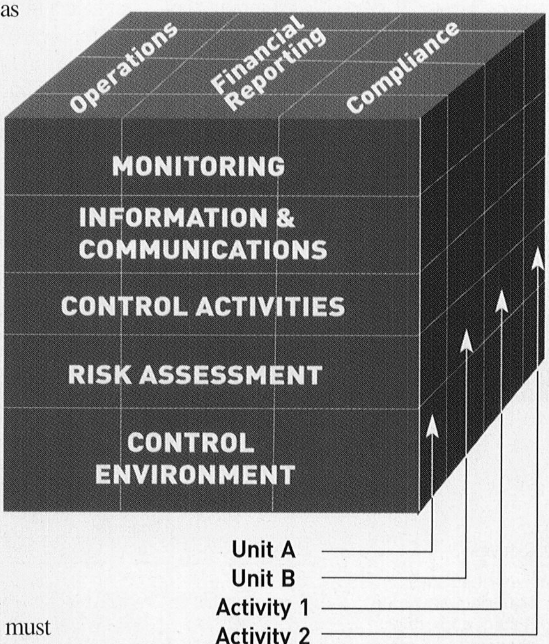
The conceptual underpinnings of the COSO framework are quite simple and based upon the following observations:

- ■ Every business has numerous operational objectives that it must accomplish in order to be successful.
- ■ Every operational objective contains various inherent quantitative and qualitative risks to its achievement.
- ■ The potential consequences of these risks should be reduced, wherever possible and practical, by instituting "integrated" internal controls.

COSO defines five key elements of an integrated, or comprehensive, framework of internal control as follows:

- ■ ***Control environment.*** Executive management and corporate governance bodies must ensure that appropriate corporate ethics and values are established and enforced at the executive level and effectively instilled throughout the entire organization. If this "tone at the top" is not successfully established, the entire system of internal control can be easily undermined and susceptible to fraud and inaccurate financial reporting.
- ■ ***Risk assessment.*** Efforts must be made to analyze, define, and document the qualitative and quantitative risks for all key business units and processes involved in achieving the organization's business objectives. Accurate risk assessment is perhaps the most critical element in establishing an effective framework of internal control. It serves to highlight and isolate those specific business units and processes which present the greatest risk to the organization's operational goals, and thereby helps focus and prioritize the creation of the organization's overall internal control framework.
- ■ ***Control activities.*** Once all internal control objectives have been established and their risks have been accurately assessed, specific safeguards, processes, and procedures must be developed and implemented to reduce or mitigate the defined risks to all critical internal control objectives. Many internal control analysis, testing, and reporting functions tend to focus almost exclusively upon control activities, because they lend themselves to objective analytical criteria. The danger, however, is that effective control activities in and of themselves do not ensure that the organization has implemented an effective system of internal controls. All five COSO components must be present to ensure that these control activities function correctly and consistently over time.

EXHIBIT 1
COSO CUBE DIAGRAM



- ■ ***Information and communication.*** Information and communication channels that support internal control objectives must be available and understood by all members of the organization as well as all necessary external entities (e.g., boards of directors, audit committees). Open internal and external communications are vital to internal control because they support the checks and balances that ensure the integrity of the control environment as well as the effectiveness and consistent application of control activities.

- ***Monitoring.*** The organization must ensure that all internal control objectives are continuously monitored, regularly tested, and revised as necessary to support changing business conditions. An effective internal control system must be dynamic and adaptable. As business technology continues to evolve, the pace of business grows exponentially faster and becomes more difficult to control. If the organization does not have a methodology in place for accurately measuring and benchmarking the effectiveness of its internal control procedures over time, these controls can quickly become outdated and ineffectual.

COSO affirms that an integrated internal control framework must take all of these elements into account and include control objectives that effectively address each of them. In other words, the effectiveness of a company's overall system of internal controls could be severely compromised if any one of these five key components is lacking in its design or execution.

COSO also requires that the development of control objectives incorporate a scope that encompasses the following three functional considerations:

- ***Operations:*** Improved operational efficiencies.
- ***Financial reporting:*** Accuracy and timeliness of the financial reporting process.
- ***Compliance:*** Adherence to all corporate legal and regulatory responsibilities.

Finally, COSO requires that control objectives based upon the guidelines detailed above be developed for all business units as well as all key business processes conducted within these units. This ensures that the control framework is designed to encompass both company-wide and process-specific operational control objectives. (*Exhibits 1* and *2* present a graphical representation of the COSO framework and an example of typical COSO internal control documentation.)

IT Support

While most IT departments are actively engaged in supporting their organization's internal controls over financial reporting, and many do so effectively, few are well versed in the disciplines and procedures necessary to adequately substantiate or document these activities in accordance with COSO or SOA requirements. This presents a significant dilemma because, in most public companies, IT departments bear a great deal of responsibility for ensuring the accuracy, integrity, and availability of the transactional data used in financial statements.

The PCAOB has recommended that in making a determination regarding which controls should be tested for Sarbanes-Oxley compliance, auditors must consider "controls, including information technology general controls, on which other controls are dependent" (PCAOB Release 2003-17).

By and large, most auditors already have some experience analyzing IT "application-level" internal controls; analysis of these controls has been included in standardized audit procedural guidelines for a number of years and has already been incorporated into the testing and walk-through procedures typically conducted during the course of a normal audit. Analyzing "general" IT controls, however, requires a level of IT knowledge and technical expertise that goes well beyond what most internal and external auditors have been trained for.

General IT controls can potentially encompass the entire spectrum of an organization's IT operations, and many of these controls, along with the systems which support them, may not be adequately documented for purposes of SOA compliance. The auditor's judgment and discretion must be

EXHIBIT 2
SAMPLE COSO INTERNAL CONTROL DOCUMENTATION

Risk Assessment and Control Activities Worksheet
Activity: *INBOUND*

	Risk Analysis				
Objectives	Risk Factors	Likelihood	Actions, Control Activities, Comments	Other Objectives Affected	Evaluation and Conclusion
Manage Logistics 1. Materials are to be tested, and either accepted and moved to storage, or rejected and returned for credit on a timely basis.	Receipt of large quantities of materials may delay the receiving and testing activities.	Medium-High	Production provides a weekly report of those items most critically needed to continue efficient and uninterrupted production. The Director of Procurement/Receiving reviews materials to be tested and prioritizes such materials based on the weekly report.		Policies and procedures are insufficient for timely processing. Policies and procedures must be developed to detail how materials should flow through receiving and testing, in the event of large amounts of materials being received, and how achievement of the objective is to be monitored. Additionally, using engineering personnel to test materials may create conflicts between testing and engineering, especially if such use negatively affects achievement of engineering objectives. Controls are sufficient to achieve the objective.

applied in order to segregate those general IT controls which could potentially have a significant or material impact on any given company's financial reporting processes. Once these high-risk controls have been successfully isolated, auditors should be prepared to provide guidance to IT department management and personnel in developing appropriate IT general control documentation and testing procedures to support ongoing SOA compliance activities.

The Changing IT Environment

Unfortunately, the COSO *Internal Control–Integrated Framework* provides little guidance regarding general IT controls, because IT environments have changed dramatically since its publication. When COSO's integrated framework was initially released, the typical enterprise IT environment was centralized and composed primarily of customized, legacy business applications. The most significant risks these systems represented to the integrity of financial data and reporting related to internal controls over application development, data entry, and system access.

In the COSO framework example documentation itself, only a handful of pages deal specifically with internal controls over IT operations, and these are nearly exclusively devoted to the aforementioned controls. While these IT internal control issues still exist and are a key focal point in any SOA control analysis, they represent only the tip of the iceberg with respect to today's financially relevant general IT controls.

Since the introduction of COSO's *Internal Control–Integrated Framework*, enterprise IT environments have grown exponentially more complex and decentralized. Sophisticated e-mail systems and web-based technologies now handle much of the financial information and corporate communications that were once conducted manually and left paper trails. Generic accounting software applications and integrated ERP systems have sophisticated financial controls that can be configured to dynamically ensure the security, availability, and integrity of financial data.

Analyzing access security parameters and data-entry batch controls is no longer enough to ensure the accuracy and integrity of a company's financial data. Modern business technologies have enabled companies to conduct transactions in real time on a plethora of disparate processing platforms. As companies continue to leverage modern business technologies, both the pace and the breadth of financial data processing continue to increase. Corralling this financial data flow will be critical to successfully controlling its accuracy and integrity in the future.

COBIT: The COSO of IT

The dizzying array of modern business technology available can differ dramatically in its potential impact on a given company, but the technology itself only represents part of the equation. What about the IT control environment is necessary to successfully manage and maintain these sophisticated IT systems?

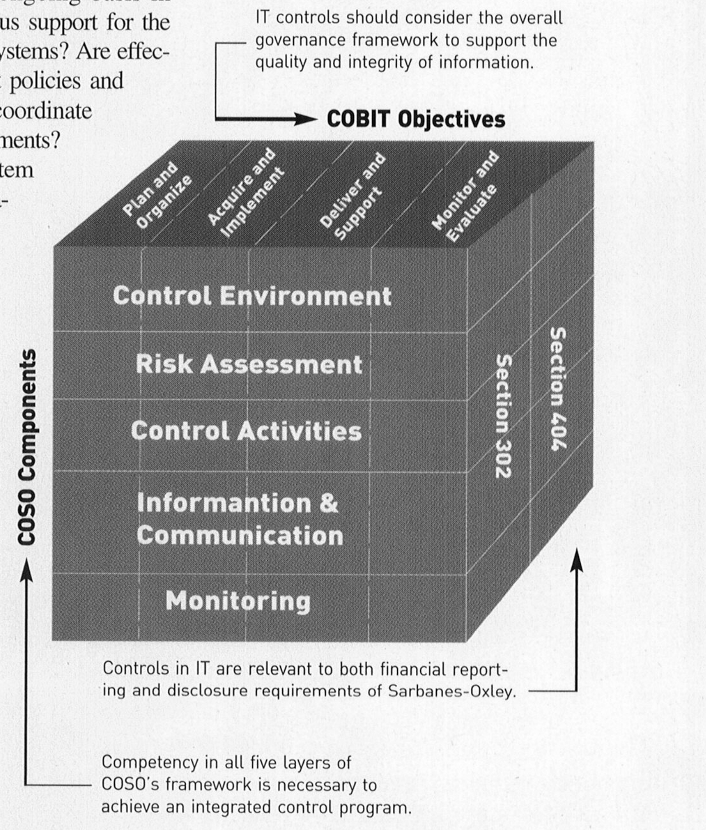
Modern IT environments often require teams of highly skilled management and technical personnel to operate efficiently. Are there enough personnel qualified to perform these duties effectively? Is their training maintained on an ongoing basis in order to ensure continuous support for the company's growing IT systems? Are effective change-management policies and procedures in place to coordinate ongoing system enhancements? Does the high-level system access to financial applications and databases that IT personnel need present a significant internal control issue?

These and countless other issues with respect to IT governance also break new ground for auditors that must now, for SOA-compliance attestation, form an opinion as to the effectiveness of the general IT controls upon which other financial internal controls depend.

The IT Governance Institute has published a discussion document, "IT Control Objectives for Sarbanes-Oxley," which provides what may be the only comprehensive methodology for assessing both general and application-level IT controls in support of SOA compliance (available from www.isaca.org). The work is based upon COBIT, a detailed set of professional guidelines for establishing effective IT governance, auditing, and internal control objectives. It identifies generic internal control objectives for the financial reporting process and modifies them accordingly to specifically address SOA compliance considerations. This specialized subset of COBIT is then mapped to the components of the COSO framework. The end result is a detailed IT internal control checklist that can be used to thoroughly assess both IT general and application-level controls for purposes of SOA-compliance analysis.

In addition to this checklist, this document also provides IT management with a comprehensive road map for coordinating all aspects of their department's support for the company's overall SOA compliance activities. Beyond being an excellent guideline for educating IT management and personnel, it is also a valuable resource for auditors that wish to achieve a greater understanding of modern IT internal controls and their relevance to SOA compliance.

EXHIBIT 3


IT controls should consider the overall governance framework to support the quality and integrity of information.
COBIT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring
Section 302
Section 404
Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.
Competency in all five layers of COSO's framework is necessary to achieve an integrated control program.

Exhibits 3 and *4* illustrate COBIT's relationship to the COSO internal control integrated framework. Using COBIT as a foundation for an SOA IT internal control analysis methodology is logical because its open framework encompasses an integrated approach to enhancing enterprise IT governance and internal control that is similar to COSO's. COBIT was designed to provide a consistent set of guidelines and best practices for maintaining an enterprise IT environment, not specifically to support the accuracy and integrity of the financial systems operating within this environment.

While COBIT and the "IT Control Objectives for Sarbanes-Oxley" discussion document derived from it provide an excellent foundation, these reference documents alone cannot solve all of the problems auditors will face in determining how the numerous IT general and application-level internal controls detailed in this documentation may affect a specific organization's financial reporting processes.

Because the COBIT IT controls are exhaustive and often focused exclusively on IT-related issues, not all will have relevance to a particular company's financial reporting processes. In general, when COBIT is the reference, auditors should be prepared to make a strong case for how and why a particular IT general control chosen for analysis or testing could potentially uncover a deficiency that could have a significant or material impact on the company's financial statements. An informed determination about the IT general controls to focus on will be critical to the successful completion of an SOA audit.

Case Study

To illustrate how to isolate modern IT general controls that could have relevance to corporate financial statement processing functions, consider the following characteristics of a typical large corporation:

- The company maintains multiple national offices and distribution centers linked via WAN and VPN connections.
- All accounting, supply chain, and fulfillment operations are fully integrated via a modern, distributed ERP system that feeds financial information back to a centralized mainframe in the home office for financial processing and reporting.
- The company has internally developed an e-commerce website that generates most of its total sales orders. A high percentage of its purchasing and EDI operations are also conducted via secure trading-partner websites maintained by vendors or independent third-party service providers.
- The company distributes the majority of its internal financial reporting documentation electronically to all business units in real time via secured intranet websites and e-mailed PDF report attachments.

For a company like this, above and beyond the standard IT security, access control, and accounting process walkthroughs, attention should also be paid to the following specialized IT general and application level control areas:

Network infrastructure. In distributed IT environments, particularly those utilizing remote-access technologies, security considerations go well beyond analyzing basic network and application-level user access parameters. A thorough analysis of IT controls in this area would include a review of firewall configuration parameters, network intrusion detection and monitoring provisions, network performance monitoring activities, network configuration and administration functions, data classification and encryption standards, e-mail and antivirus filtering provisions, business continuity provisions, and critical third-party service provider reliability. Because any weak link in the chain of a company's network infrastructure could jeopardize the company's financial data, a key deficiency in this area could ultimately have a significant effect on the company's financial statement production process.

Another key issue is the role the network plays in supporting corporate communications. Information and communication represents one of the key COSO elements in establishing an integrated framework of internal control. Any significant deficiencies that could compromise reliable information exchange and corporate communications could also represent a key internal-control concern.

ERP configuration and business continuity. Modern ERP and accounting systems are capable of fully automating and integrating many highly complex business processes and centrally regulating and monitoring a broad array of financial and accounting system controls. No two vendors' ERP or accounting applications are alike, and many can be extensively customized to support specialized vertical industry require-

EXHIBIT 4
COBIT CONTROL OBJECTIVES

	COSO Component				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize					
Define a strategic IT plan.		•		•	•
Define the information architecture.			•	•	
Determine technological direction.					
Acquire and Implement					
Identify automated solutions.					
Acquire and maintain application software.			•		
Acquire and maintain infrastructure.			•		
Deliver and Support					
Define and manage service levels.	•		•		•
Manage third-party services.	•	•	•		•
Manage performance and capacity.	•		•		
Monitor and Evaluate					
Monitor the processes.				•	•
Assess internal control adequacy.					•
Obtain independent assurance.	•				•

ments. Detailed knowledge of the control, security, and workflow configuration parameters particular to the specific ERP and accounting software applications in use is critical in analyzing how effectively these systems support the company's internal controls over financial processes and procedures.

In the example above, all internal accounting operations are being processed centrally via the home office's mainframe. This affects the company's ability to produce accurate financial reports on a timely basis should an unplanned business interruption make this system unavailable for an extended time. As a result, an IT internal-control review should ascertain whether the company has performed a formal business-impact analysis or risk-assessment study on its mission-critical business systems, and whether adequate business continuity provisions have been established.

Web-based application development considerations, and third-party reliance. As companies continue to migrate mission-critical business applications to the web and integrate web-based applications with back-end accounting systems, the technical sophistication necessary to effectively evaluate and test related internal controls has grown considerably. Companies employ dozens of different database and application development tools in building their websites. Insofar as these websites increasingly support critical financial operations that could have a material impact upon the company's financial reporting processes, they represent a key point of concern.

When analyzing web-based application development, auditors should focus on the methodology the company is employing to monitor and regulate website development and maintenance. Are these activities being properly administered, tracked, and audited? Are web-based applications tested thoroughly prior to introduction? Are encryption standards implemented to protect sensitive data? Are adequate reconciliation procedures in place to ensure that online financial transactions are correctly recorded on a timely basis in the company's back-end accounting systems? Are the underlying databases adequately secured to prevent unauthorized access and manipulation of data prior to their entry into the accounting system? Are any key third-party service providers or business partners utilized to support web-based business activities, and are their systems secure?

Paperless Financial Reporting Systems

Implementing real-time financial management and paperless reporting systems can dramatically enhance the efficiency of an enterprise's operations. While helping make companies more nimble, the increasing adoption of these technologies has robbed auditors of ready access to the paper trails that have traditionally supported their analysis and testing of internal controls.

To successfully analyze IT controls surrounding dynamic systems and paperless environments, auditors must acclimate themselves to specialized data extraction and analysis tools and work directly with the live data that reside on these systems. Walk-throughs of financial reporting functions will require a detailed understanding of the underlying databases, scripts, applications, and electronic reports generated by these systems. Auditors must also analyze the automated internal control procedures that have been programmed into these applications to perform data integrity checks, including exception handling, error tracking, and reconciliation functions, as well as the e-mail and intranet-based workflow automation processes utilized to streamline financial reporting.

While by no means exhaustive, these illustration issues identify various general IT controls that could have a material impact on financial statements. It is necessary to have a clear understanding of the relationship between these IT general controls and the financial processes they support within the organization's overall framework of internal control. ❑

Sid M. Edelstein, CPA, *is a principal and director of IT services at Cornick, Garber & Sandler, LLP, New York, N.Y. He would like to thank Malcolm Schwartz, one of COSO's original authors, for his review and comments.*