

Reducing the Threat Levels for Accounting Information Systems

Challenges for Management, Accountants, Auditors, and Academicians

By Deborah Beard and
H. Joseph Wen

One of the early actions of the U.S. Department of Homeland Security (DHS) was to develop the now-familiar color-coded security alert system: Red signaled a "severe" threat to national security, orange a "high" threat, yellow an "elevated" threat, blue a "guarded" threat, and green a "low" threat. In the wake of the recent scandals at Enron, Arthur Andersen, WorldCom, Tyco, and others, one can imagine a similar security alert system for threats to our financial reporting system.

Two possible security risk levels for financial reporting are detailed in Exhibits 1 and 2. First, consider the "Severe Security Alert Level: Code Red." At this risk level, there are serious attacks possible against our financial reporting system, financial markets, and economy. Scarce resources, including time and money, are being embezzled, misappropriated, or diverted. Investor confidence has been shaken and management has become pessimistic about the future. The government has responded with costly regulation and increased oversight of the executive management and the accounting profession. Information security is experiencing dramatically increased threats.

Now, consider the lower "Guarded Security Alert Level: Code Blue" of Exhibit 2. This risk level recognizes the importance of strong corporate governance and information security in utilizing scarce resources to increase shareholder wealth and



to regain the confidence of market participants. Financial decisions are based on accurate, transparent, and timely information that is both relevant and reliable. Investors, creditors, and other users can safely rely on financial reports to assist them in assessing the amounts, timing, and uncertainty of future cash flows, in identifying the resources and claims to those resources, and in evaluating performance. The appropriate "tone at the top" with respect to business and eth-

ical conduct is being demonstrated. Management, audit committees, accountants, and auditors are working together to continuously improve internal control and strengthen information security.

Certainly, there is reason to believe that the business environment has experienced many of the threats consistent with a Code Red. Many of these threats have provided challenges for corporate governance, accountants, auditors, and academicians. One goal

businesses hopefully have in common is reducing the threat level to our accounting information system closer to Code Blue.

Security Threats to Internet Commerce and Technology

The growth of the Internet has been fueled by its potential for conducting business. The Internet has removed physical barriers to commerce, tapping previously uneconomical markets. The power of the Internet to facilitate business can be severely offset by users' concern over security. The website problems occasionally experienced by major e-commerce providers such as Yahoo, eBay, E-Trade, and Amazon.com have provided evidence of some of the risks of Internet-based attacks.

The use of Internet technologies has substantially increased the vulnerability of information systems. One of the fastest-growing threats on the Internet is the theft of sensitive financial data. Failure to include basic information security unwittingly cre-

ates significant business and professional risks. For example, without effective security, a hacker may be able to access user passwords, providing entree to an array of system capabilities and information. Such breaches can have serious legal consequences. Or, trade secrets may be uncovered and disseminated, diminishing competitive advantage and profits.


Inadequate information security increases the opportunity for manipulation, falsification, or alteration of accounting records. Unauthorized or inappropriate access to the accounting information system, or the failure to establish and maintain separation of duties as part of a system of internal control, may make it difficult to ensure that valid and accurate transactions are recorded, processed, and reported. There are a number of threats to accounting information systems, especially for those systems used in conjunction with the Internet. These threats represent challenges to management, accountants, auditors, and academicians.

Threats to Accounting Information Systems

Threats to accounting information systems come from a variety of sources. If ignored, they can destroy the relevance and reliability of financial information, leading to poor decisions by various stakeholders. (For specific examples, the *Sidebar* lists the top 10 concerns identified by a 2006 AICPA survey.)

At the point of data collection, it is important to establish security controls that ensure that transaction or event data are valid, complete, and free from material errors. Masquerading (pretending to be an authorized user) and piggybacking (tapping into telecommunications lines) are examples of hacker activities that can seriously impact valid data collection.

Threats to accounting information systems can also occur during the data processing phase. Creating illegal programs, accessing or deleting files, destroying or corrupting a program's logic through viruses, or altering



Mark Your Calendar!

Personal Financial Planning and Eldercare Joint Conference

Wednesday, June 20, 2007
The New York Helmsley Hotel
212 East 42nd Street
New York, NY 10017


Let FAE help you manage and preserve your clients' wealth.

Invited speaker, **Conrad DeQuados**, Senior Economist and Managing Director, Bear Stearns & Co., Inc., will present an "Economic Update."

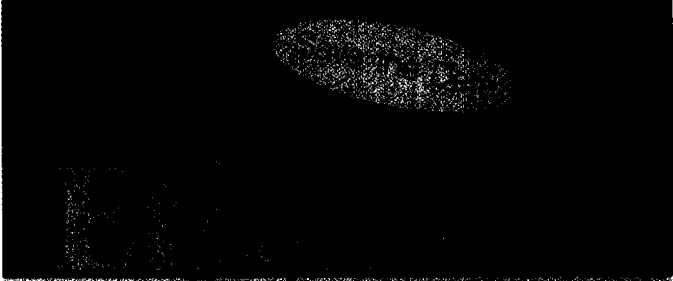
Session Topics Include:

- Financial Planning in the 21st Century
- Eldercare and Medicaid Update: Parts I and II
- The Top Ten Insurance Planning Techniques
- Over six concurrent topics, including IRA Planning, Geriatric Care, and more

This program satisfies requirements for CPE recertification credit. Participants can earn 8 credit hours by attending. This program has been accepted by the CFP® Board for 8 CE credit hours.

Foundation for Accounting Education

Foundation for Accounting Education

Register at www.nyacpa.org or call 1-800-537-3635




Conference

This conference will benefit you with the latest trends in research, planning, and administration. It will also make your practice more successful.

<p>Thursday, July 21, 2007 FAE Conference Center 3 Park Avenue, 14th Floor New York, NY 10016</p>	<p>Friday, July 22, 2007 Marriott Marquis Hotel 1230 Avenue of the Americas New York, NY 10020</p>
--	---

Highlights:

- Guidelines for Writing a Code of Ethics
- Ethical Issues for Practicing Accountants
- Employment Law Update for Public Accounting Firms
- Where Ethics and Liability Cross
- Ethics and Nonprofit Leaders

Foundation for Accounting Education

Foundation for Accounting Education

a program's logic to cause the application to process data incorrectly all represent threats. Threats to database management might include unauthorized access that allows altering, deleting, corrupting, destroying, or stealing data. The failure to maintain backup files or other retrieval techniques represents a potentially devastating loss of data. Threats to the information generation and reporting phase must also be considered. For example, the theft, misdirection, or misuse of computer output could damage the competitiveness or reputation of the organization.

Advances in information technology and increased use of the Internet require that management, accountants, auditors, and academicians become more knowledgeable and conversant in the design, operation, and control of accounting information systems.

Implications for Management

With the expansion of computer technology, traditional business processes have

been restructured and unique internal control techniques are required to address exposure to many new dangers. The responsibility for establishing and maintaining a system of effective internal controls resides with management. Management's responsibilities include the documentation, testing, and assessment of internal controls, including relevant general IT controls (e.g., program development, program changes, computer operations, and access to programs and data) and appropriate application-level controls designed to ensure that financial information generated from an organization's information system can be reasonably relied upon (see www.sec.gov).

The Foreign Corrupt Practices Act of 1977 and the Sarbanes-Oxley Act of 2002 (SOX) assign important legal responsibilities to management. Management and other personnel are expected to provide reasonable assurance annually regarding the reliability of financial reporting and the prepara-

tion of financial statements for external purposes in accordance with GAAP. Management is expected to establish, evaluate, monitor, and provide written assessments of internal controls, which include policies and procedures that—

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and disposition of the assets of the registrant;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorization of management and directors of the registrant; and
- provide reasonable assurance regarding the prevention or timely detection of any unauthorized acquisition, use, or disposition of the registrant's assets that could have a material effect on the financial statements (www.sec.gov).

Section 404 of SOX mandates a statement of management's responsibility for establishing and maintaining adequate internal controls over financial reporting and an assessment of the effectiveness of those internal controls: preventive controls, which include techniques designed to reduce the frequency of undesirable or devastating actions; detective controls, which include devices, techniques, and procedures designed to expose undesirable or devastating actions that elude preventive controls; and corrective controls, which involve actions to reverse the effects of undesirable or potentially devastating actions.

SOX does not mandate a single particular form of documentation of internal control compliance; the extent of documentation may vary, depending upon the size and complexity of the organization. Documentation might be paper or electronic, and can include a variety of information, including policy manuals, process models, flowcharts, job descriptions, documents, and forms. Inadequate documentation of the design of controls over relevant assertions related to significant accounts and disclosures is, however, considered a deficiency in the company's internal control system. COSO (www.coso.org), COBIT (www.isaca.org), ISO (www.iso.org), and SysTrust (www.

EXHIBIT 1

Severe Security Alert Level: Code Red

- The accounting information system has been attacked; it is impossible to see the true economic and financial activities of the organization. Unauthorized or inappropriate access to information systems increasingly makes it difficult to ensure that appropriate transactions are recorded and reported.
- Scarce resources are being embezzled and misappropriated by executive management and other employees. Top executive managers are being charged with stealing tens of millions of dollars, violating securities laws, and committing fraud and conspiracy by inflating earnings.
- Investor confidence, already shaken by significant volatility in the capital markets, has been further unsettled by highly publicized restatements of financial statements, which have generated questions about the quality of financial reporting, the effectiveness of the independent audit process, and the efficacy of corporate governance.
- Excessive, costly regulation has been necessary to provide oversight and penalties for fraud and other malfeasance. Reported costs of compliance have exceeded \$35 billion.
- Business management personnel are pessimistic, resulting in a significant decline in capital investment spending and increased unemployment rates.
- Earnings and share prices have nosedived; financial wealth has declined by trillions.
- Increased pressures on management to maintain or achieve financial targets have heightened the risk of improper accounting or failure to disclose related party transactions.
- Future financial stability and plans have been devastated.

systrustservices.com) have provided useful frameworks and principles for documenting controls.

Management must ask important questions and be able to rely on the answers with confidence:

- Did assets, liabilities, and other elements shown on financial statements actually exist?
- Did recorded transactions included in the financial statements actually occur?
- Did the financial statements include all transactions and accounts that should be presented?
- Were accounts included in the financial statements at appropriate values?
- Are the assets shown on the balance sheet rights of the company?
- Are the liabilities shown on the balance sheet obligations of the company?
- Are elements of financial statements appropriately classified and disclosed?

How much reliance can be placed on the answers if a significant information security threat exists and management has not taken appropriate measures to protect the organization from internal and external attacks?

Implications for Accountants and Auditors

Accountants—as users, managers, designers, and evaluators of information systems—should be knowledgeable of security threats and appropriate control techniques in order to protect their own information systems and to advise businesses about security risks. A company's use of information technology and the security of the accounting information system affect the company's internal control over financial reporting. System processes and system-generated entries for valid transactions and events are an integral part of financial reporting. Since the advent of computer systems that capture, verify, store, and report the data used in financial reports, new security issues involving technology have developed.

Although SOX prohibits auditors from offering information system design and implementation services to audit clients, SOX mandates that every independent audit report include an auditor attestation report relating to the internal control assessments made by management. Specific notation of any significant defects or material

noncompliance must be included in that report. In addition, the New York Stock Exchange now requires all listed companies to maintain an internal audit function to provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control.

Auditors are also facing increased challenges from several recent Statements on Auditing Standards (SAS), especially SAS 94 and the new audit risk standards (SAS 104–111) that have been issued by the AICPA's Auditing Standards Board (ASB). These SASs establish standards and provide guidance concerning the auditor's assessment of the risk of material misstatement (whether caused by error or fraud) in a financial statement audit, and the design and performance of audit procedures whose nature, timing, and extent are responsive to the assessed risks. Auditors are required to gain a better understanding of the entity and its environment, including internal con-

trols, in order to identify the risks of material misstatement in the financial statements and what the entity is doing to reduce the risks; conduct a more rigorous assessment of the risks of misstatement of financial statements based on that understanding; and improve the linkage between assessed risks and the nature, timing, and audit procedures performed in response to those risks. The auditor must plan and perform the audit to obtain sufficient evidence that audit risk will be limited to a level that is, in his or her professional judgment, appropriate for expressing an opinion on the financial statements with "reasonable assurance."

Adoption of new technologies and new or revamped information systems is an emerging risk in today's business environment. The proliferation of computer-based information systems has had a tremendous impact on the business environment and the auditing of entities where IT has been integrated into operations and information systems. Internal and

EXHIBIT 2

Guarded Security Alert Level: Code Blue

- Public trust in financial reports and in the statements issued by corporate management is widespread; reported financial information is accurate, transparent, relevant, reliable, and timely.
- Investors, creditors, and other users can rely on financial reports to assist them in assessing future cash flows, the resources and claims to resources, the results of operations, and changes in equity.
- Scarce resources are being used by managers to increase shareholder value rather than to comply with excessive regulation.
- Individuals comply with rules, regulations, and laws and demonstrate high standards of business and ethical conduct. Management sets the appropriate tone at the top.
- Managers, audit committees, boards of directors, auditors, and regulators work together to "connect the dots" and determine deficiencies in internal control and other threats to the accounting information system.
- Effective access security controls provide a reasonable level of assurance against inappropriate access and unauthorized use of systems, and intercept hackers, malicious software, and other intrusion attempts. Secure passwords, Internet firewalls, data encryption, and cryptographic keys prevent unauthorized access. Access privilege controls restrict the applications to authorized users, supporting an appropriate division of duties. There are frequent and timely reviews of the user profiles that permit or restrict access.
- Management and other market participants are optimistic about the future while remaining vigilant to threats.

external auditors are increasingly involved in IT audits and in assessing the effectiveness of internal control. Auditors must recognize that the increased use of IT requires assessments of the potential impact on internal control and in the planning and completion of the auditing process. Attesting to the integrity of data collection, data processing, database management, and information generation has become more complicated as the fundamental ways in which transactions are initiated, recorded, processed, and reported have changed. Ineffective controls on IT provide serious threats to internal control. For example, unauthorized access to software and data can lead to unauthorized, nonexistent, or inaccurate transactions.

SAS 94 specifically requires auditors to consider the effect of IT on internal con-

The proliferation of computer-based information systems has had a tremendous impact on the auditing of entities where IT has been integrated into operations and information systems.

trol and audit evidence, providing guidance on collecting sufficient, competent evidence and identifying circumstances when the system must be accessed in evaluating controls and assessing control risk. An auditor must understand the design of controls, determine whether the controls are in place, and evaluate the effectiveness of the controls. An entity's use of IT and manual procedures may affect controls relevant to the audit, and should be considered. An auditor then assesses control risk for the assertions embodied in the account balance, transaction data, and disclosure components of the financial statements. An auditor should obtain evidence of the effectiveness of the design and operation of controls to reduce the assessed level of control risk.

An auditor uses the understanding of internal control and the assessed level of control risk in determining the nature, timing, and extent of substantive tests for financial statement assertions. As an entity's operations and systems become more complex, it becomes more likely that the auditor would need a greater understanding of internal control components to design tests of controls and substantive tests.

SAS 94 clarifies the controls needed to ensure that recurring and nonrecurring entries are authorized, complete, and correctly recorded in an IT environment. The auditor should obtain an understanding of how IT affects control activities relevant to planning an audit. Application controls entail the use of IT to initiate, record, process, and report transactions or other financial data. Examples include edit checks of input data, numerical sequence checks, and manual follow-up of exception reports. General controls are policies and procedures that support the effectiveness of applications controls by helping ensure continued proper operation of information systems. General controls commonly include controls over data center and network operations; system and application acquisition and maintenance; access security; and application system acquisition, development, and maintenance. Examples of general controls include controls that restrict access to programs or data, controls over the implementation of new releases of packaged software applications, and controls over system utilities that could change financial data or records without leaving an audit trail.

SAS 94 identifies potential benefits from IT in the effectiveness of internal controls, including: consistent application of business rules and performance of complex calculations; enhanced timeliness, availability, and accuracy of information; and enhanced ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems. SAS 94 also recognizes, however, that IT poses specific risks to internal control, including the reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both; unauthorized access to data that may result in destruction of data or improper changes to data, including nonexistent or inaccurate transactions; and potential loss of data. SAS 94 also stresses that more-

extensive documentation (e.g., flowcharts, questionnaires, or decision tables) may be necessary to support an auditor's understanding and evaluation of internal controls and IT risk assessments.

SAS 94 provides guidance in assessing when specialized skills are required to consider the effect of IT on the audit, to understand controls, and to design and perform audit procedures. Factors to be considered by an auditor in determining whether a specialist is needed are: the complexity of the entity's systems and IT controls, and the manner in which they are used in conducting the entity's business; the significance of changes to existing systems or the implementation of new systems; the extent to which data are shared among systems; the extent of the entity's participation in electronic commerce; the entity's use of emerging technologies; and the significance of electronic-only audit evidence. According to SAS 94, procedures that the auditor may assign to an IT professional include: inquiring how data and transactions are initiated, recorded, processed, and reported; how IT controls are designed; inspecting systems documentation; observing the operation of IT controls; and planning and performing tests of IT controls. An auditor should have sufficient IT knowledge to communicate the audit objectives to an IT professional, to evaluate whether procedures will meet the auditor's objectives, and to evaluate the results of the procedures as they relate to the nature, timing, and extent of other audit procedures.

Information systems auditors, who evaluate how a company's computer systems safeguard assets and maintain data integrity, are in hot demand. *The Wall Street Journal* reported in May 2006 that more employers are requesting professional certifications as a way to indicate high skill levels and show SOX regulators that staff are knowledgeable. Effective communication and strategies among management, accountants, and auditors are important in reducing or defending against emerging threats to the accounting information system.

New auditing techniques for evaluating internal controls and verifying the reliability and credibility of the data from the accounting information system have been and will continue to be needed. To properly evaluate the potential risks, accountants and auditors must be familiar with

TOP 10 TECHNOLOGY CONCERNS

C PAs have consistently recognized the potential for threats and opportunities for shielding individuals, organizations, and business and accounting professionals from attacks. The results of the AICPA 2006 Top Ten Technologies survey noted the following issues of greatest concern:

- **Information security:** the hardware, software, processes, and procedures in place to protect information systems from internal and external threats. They include routers, perimeter firewalls, IP strategy, intrusion detection and reporting, content filtering, antivirus, antispyware, password management, vulnerability assessment, patch management, personal firewalls, wireless security strategies, data encryption, locked facilities, and user education.
- **Assurance and compliance applications** (e.g., SOX section 404, enterprise risk management): collaboration and compliance tools that enable various stakeholders to monitor, document, assess, test, and report on compliance with specified controls.
- **Disaster and business continuity planning:** the development, monitoring, and updating of the process by which organizations plan for continuity of their business in the event of a loss of information resources due to theft, virus infection, weather damage, accidents, or other malicious destruction.
- **IT governance:** the structure of relationships and processes to direct the enterprise in order to achieve the enterprise's goals by adding value while still balancing risk versus return over IT and its processes.
- **Privacy management:** the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information. As more information and processes are being converted to a digital format, this information must be protected from unauthorized users and from unauthorized usage by those with access.
- **Digital identity and authentication technologies:** ways to ensure users are who they say they are. These include hardware and software solutions that enable the electronic verification of a user's identity or a message's validity through, for example, digital certificates. This technology includes the use of bar codes, magnetic stripe, biometrics, and tokens, as well as access control for authentication, nonrepudiation, and authorization.
- **Wireless technologies:** connectivity and transfer of data between devices via the airwaves (i.e., without physical connectivity). Wireless technologies include Bluetooth (PAN), infrared, WiFi (802.11 WLAN), WiMax (802.16), 2.5 G and 3G (WWAN), and satellite.
- **Application and data integration:** using current and emerging technologies, including .NET, web services, Java, XML (the foundation for XBRL), and Ajax, to facilitate integration of data between heterogeneous applications. In its most basic format, XBRL focuses on improving the gathering, analyzing, sharing, and synchronizing of business reporting data. This allows organizations to select "best of breed" applications that can be seamlessly integrated.
- **Paperless digital technologies:** document and content management, including the process of capturing, indexing, storing, retrieving, searching, and managing documents electronically (PDF and other formats), including database management. Knowledge management then brings structure and control to this information, allowing organizations to harness the intellectual capital in the underlying data.
- **Spyware detection and removal:** technology that detects and removes programs attempting to covertly gather and transmit confidential user information. Spyware applications are typically bundled as a hidden component of freeware or shareware programs, or attached to malicious websites. Once installed, spyware can monitor user activity, gather information about e-mail addresses, passwords, and credit card numbers in the background, then transmit the information to someone else. Spyware can include remote access trojans (RAT) and root kits.

Source: AICPA News Release: January 31, 2006; infotech.aicpa.org/Resources

current and emerging technologies. Controls over unauthorized access to accounting records are important components of internal control. Access and password policies, encryption, digital signatures, disk locks, firewalls, and digital certificates are examples of control measures that should be identified, documented, reported, and subjected to verification in an evaluation of control effectiveness.

Professional development in documenting internal control, compliance, and the impact of IT is available through a number of organizations. Information can be found from the SEC (www.sec.gov), AICPA (www.aicpa.org), IIA (www.theiia.org), IMA (www.imanet.org), COSO (www.coso.gov), and ISACA (www.isaca.org).

Implications for Academics

Are educators providing students with a framework for understanding the need for IT security and the importance of working with others to develop policies, pro-

cesses, and technology to address the threats? Do future accounting professionals have the opportunity to learn about information security, assurance and compliance applications, business continuity planning, IT governance, privacy management, digital identity and authentication technologies, application and data integration, new wireless and paperless technologies, and spyware detection and removal? Are accounting majors required to demonstrate the knowledge, skills, and ethics that will enable them to understand business environments, make risk assessments, evaluate internal controls, and implement effective and efficient security measures?

Academics, especially teachers of accounting, MIS, IT, and related business topics, should work together to ensure that future professionals have the knowledge, skills, and abilities to work as managers, accountants, or auditors to address continuing threats. Seeking integration of

security topics and techniques into accounting curricula is important; working across disciplines appears critical. Recognizing and rewarding faculty activities and accomplishments in cross-functional curriculum development, professional growth, and professional service through promotion and tenure decisions is important.

It should be noted that the CPA, CMA, and CIA certifications have increasingly recognized the importance of IT. On the CPA exam, 12% to 18% of the "Auditing and Attestation" section and 22% to 28% of the "Business Environment and Concepts" section test topics relate to computerized environments and IT implications in the business environment. On the CMA exam, 15% of Parts I and II relates to risk assessment, internal control, systems controls and security, systems development and design, electronic commerce, enterprise resource planning (ERP) systems, and other areas relating to information systems and technology.

Save
the Date

IRS

Practice and Procedures Conference

Offering tips, strategies, and objectives to communicate effectively with the IRS

Thursday, June 28, 2007

New York Helmsley Hotel
212 East 42nd Street
Between 2nd and 3rd Avenues
New York, NY 10017

Course Code: 25609811
Member Fee: \$350
Nonmember Fee: \$450
CPE Credit Hours: 8

Topics Include:

- ▶ E-File Services: Large and Medium-Sized, Small and Self-Employed Businesses
- ▶ Compliance Regulations
- ▶ Taxpayer Advocate and Practitioner Priority Services
- ▶ Current Events in Appeals

And more!

Foundational for Accountability
FAE
Education

For more information, visit www.nysscpa.org or call 800-537-3635.

Back by Popular Demand

POP

POP PASS HOLDER BENEFITS INCLUDE:

- ▶ Pay One Price & Enjoy Incredible Savings
- ▶ Convenient Online Registration for Events
- ▶ No Surcharges
- ▶ Valid Until August 31, 2007

FOLLOW THESE EASY STEPS TO ENROLL TODAY:

- ▶ Visit www.nysscpa.org for a registration form, and return it with payment to the address indicated, or fax it to FAE at 212-719-3365.
- ▶ Or call 800-537-3635 to enroll by phone.

Individual Price	\$1,350
Firm/Company Price	\$2,350

For more information regarding POP Pass Administrative & Registration guidelines, log on to <http://www.nysscpa.org/faeorg/popguidelines.htm>

FAE's Pay-One-Price Discount Program, designed for individual members and companies, is the most affordable approach to obtaining the highest-quality FAE CPE.

Foundational for Accountability
FAE
Education

On the CIA exam, 30% to 40% of Part III covers IT, including control frameworks, data and network communications, electronic data interchange, encryption, and information protection.

tions, as well as providing them with a conceptual understanding of the interrelationship of internal control, information security, financial reporting, and IT-related security and control measures, is impor-

in keeping accounting information systems safe.

Safeguarding personal and proprietary information and ensuring the integrity of the components of the accounting information system in today's digital environment present many challenges. Implementation of effective information system requirements should provide reasonable assurance that the accounting information system will produce relevant and reliable information to meet internal and external reporting needs.

With or without SOX, internal control must be a top priority. Policies and procedures should require the maintenance of records that accurately detail and fairly reflect transactions and dispositions of assets; provide reasonable assurance that transactions are recorded properly; ensure that receipts and expenditures are made only in accordance with proper authorization; and provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use, or disposition of assets that could have a material effect on the financial statements.

Identifying, implementing, and monitoring some basic system requirements and sustainable solutions for both the general and unique security challenges that can arise in an unbounded electronic enterprise with a technologically rich environment should be undertaken. These include policies and procedures related to e-mail passwords and usage, antivirus and antispyware solutions, firewalls, authorized access, authentication, separation of duties, privacy, encryption, digital signatures and certificates, non-repudiation, data integrity, storage, backup files and tapes, and other emerging threats and technologies. Finally, the establishment of the right tone at the top with respect to privacy and security, as well as the hiring of vigilant, ethical employees, is essential to securing our information system against dangerous threats. □

Deborah Beard, PhD, CMA, is an associate professor, and H. Joseph Wen, PhD, is a professor, both in the department of accounting and MIS, Harrison College of Business, Southeast Missouri State University, Cape Girardeau, Mo.

Safeguarding personal and proprietary information and ensuring the integrity of the components of the accounting information system in today's digital environment present many challenges.

Newer professional designations, such as the Certified Information Technology Professional (CITP), Certified Information Systems Auditor (CISA), and Certified Information Systems Security Professional (CISSP), demonstrate the demand for certifications related to information technology, systems auditing, and systems security. For example, ISACA had 31,000 people sign up to take the CISA in 2005, twice the number in 2004.

Informing students of the changing content and growth of professional certifica-

tion. In addition, academics will need to help future accounting professionals recognize that they must be committed to lifelong learning and staying abreast of these and other issues in the future.

Understanding the Need for Security: A Common Denominator

The security of electronic information has become a critical concern. Academics, managers, accountants, and auditors must all be conversant with emerging threats and security measures that are effective

FOR FURTHER READING

AICPA, *Top Ten Technologies Survey*, www.aicpa.org/infotech/technologies/toptechs.htm.

AICPA, *Summary of the Eight Audit Risk Assessment Standards, SASs 104-111*, www.aicpa.org/risk.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, AICPA, 1992.

James A. Hall, *Accounting Information Systems*, 4th Edition, Thomson South-Western, 2004.

IT Governance Institute, *Control Objectives for Information and Related Technology (COBIT)*, www.isaca.org.

Sarah E. Needleman, "Sarbanes-Oxley Creates Special Demand," *Wall Street Journal*, May 16, 2006, B8.

Public Company Accounting Oversight Board (PCAOB), *Auditing Standard 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, June 5, 2006.

SEC, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," Release Nos. 33-8238; 34-47986; IC-26068; File Nos. S7-40-02; S7-06-03, www.sec.gov/rules/final/33-8238.htm