Internal Controls: The Key to Accountability*

*connectedthinking

PRICEWATERHOUSECOOPERS

PRICEWATERHOUSECOOPERS

Internal Controls: The Key to Accountability

By John A. Mattie, Paul F. Hanley, and Dale L. Cassidy

About the Authors

John A. Mattie is PricewaterhouseCoopers' National Education & Nonprofit Practice Leader. He has over 25 years of diversified audit and consulting experience with particular expertise serving public and private research universities as well as independent schools and other types of not-for-profit organizations. Previously, John led PricewaterhouseCoopers' education consulting practice. His current role combines his audit and consulting leadership skills.

Paul F. Hanley is a PricewaterhouseCoopers audit partner who specializes in serving colleges, university, not-for-profit and government organizations. He is one of the Firm’s top national technical consultants, especially concerning issues affecting public colleges and universities.

Dale L. Cassidy is a director in PricewaterhouseCoopers’ Education Advisory Services practice. He specializes in advising colleges and universities about risk and control issues, such as those raised by the Sarbanes-Oxley Act of 2002.

The authors have written numerous publications including:

- The upcoming second edition of ***Understanding Financial Statements: A Strategic Guide for Independent College and University Boards*,** which is expected to be published by the Association of Governing Boards of Universities and Colleges (AGB) in 2005
- ***Meeting the Challenges of Alternative Investments***, published by PricewaterhouseCoopers in 2004
- ***The Changing Role of the Audit Committee: Leading Practices for Colleges, Universities and Other Not-for-Profit Educational Institutions***, published by PricewaterhouseCoopers in 2004
- ***A Foundation for Integrity***, published by PricewaterhouseCoopers in 2004
- **"The Substance of Transparency: The Sarbanes-Oxley Act,"** published in the February 2003 edition of the National Association of College and University Business Officer’s (NACUBO’s) magazine, *Business Officer*
- ***Developing a Strategy To Manage Enterprisewide Risk in Higher Education*,** published by NACUBO in 2001
- ***GASB 35 Implementation Guide - Questions and Answers for Public Colleges and Universities Using BTA Reporting,*** which was published by NACUBO and PricewaterhouseCoopers in 2001

About PricewaterhouseCoopers

PricewaterhouseCoopers is a leading provider of professional services for colleges and universities. Our goal is to help our higher education clients turn their complex business issues into opportunities and measurably enhance their ability to build value, manage risk and improve performance.

For more information about our higher education services, call us in the U.S. at 1-888-272-3236 or visit our Web site at **http://www.pwc.com/education**.

PricewaterhouseCoopers (**www.pwc.com**) provides industry-focused assurance, tax and advisory services for public and private clients. More than 120,000 people in 139 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

"PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

Table of Contents

I. Introduction

Internal controls are essential to the success of the business operations of colleges and universities, including those with academic medical centers (AMCs), and other not-for-profit educational institutions. Internal controls assist board members and management in carrying out their fiduciary duties and operating responsibilities. They help to:

- Facilitate the preparation of timely and accurate financial reports and information
- Ensure that the institution complies with applicable federal and state laws and regulations
- Foster effective and efficient campus operations

Questions?
Please call us in the U.S. at 1-888-272-3236 or visit our website at: www.pwc.com/education.

Internal controls are receiving greater attention because of corporate financial scandals and the resulting passage of the Sarbanes-Oxley Act of 2002 (Sarbanes), which established new or enhanced standards of corporate accountability.[1] Although Sarbanes is not applicable to colleges, universities, AMCs and other not-for-profit organizations, it is focusing greater attention on their internal controls as well as their governance and management practices. This increased attention comes not only from boards of directors and governmental and private funding sources, but increasingly from legislative entities as well.

At the state level, the Attorney General (AG) of New York, Eliot Spitzer, is encouraging directors of not-for-profit organizations to pay more attention to internal controls. The booklet, *Internal Controls and Financial Accountability for Not-for-Profit Boards,* that his office recently published notes:

> "A primary responsibility of directors and officers is to ensure that the organization is accountable for its programs and finances to its contributors, members, the public and government regulators…The development and maintenance of the organization's internal controls will help to ensure accountability." [2]

Under existing laws in many states, AGs or other state officials are responsible for monitoring the activities of public charities with regard to the solicitation of funds from the public as well as the management of institutional funds (e.g., the Uniform Management of Institutional Funds Act or UMIFA). Several AGs and legislatures have made or are considering changes to the laws that apply to not-for-profit organizations within their state borders. Most apply to fundraising activities, but a few of the proposed laws would impose new requirements for directors and officers designed to enhance their accountability.

For example, California passed the *Nonprofit Integrity Bill* in 2004, which became effective on January 1, 2005. It requires certain large charities—but not colleges, universities and AMCs—to have audit committees. However, other requirements in the *Bill*, such as requiring board approval of the President's and Chief Financial Officer's or Treasurer's compensation packages, apply to colleges, universities and AMCs. [3]

Iowa also passed new legislation affecting charities in 2004. The *Revised Iowa Nonprofit Corporation Act* became effective on January 1, 2005. Iowa's revised act establishes standards of conduct for directors—they must act in good faith and in a manner that they reasonably believe is in the best interests of their organizations. Also, the act establishes requirements for transactions in which a director has a conflict of interest. [4]

Massachusetts is expected to consider legislation this year that would affect directors and officers of the state's public charities. According to a draft by the AG's office that was released in 2004, the principal managing officers of larger charities (defined as those with annual gross revenues of $750,000 or more) would need to certify to the accuracy of financial reports submitted to the AG's office. The principals also would be required to certify that they have designed and maintained internal financial controls and disclosed to the audit committee and the charity's auditors material deficiencies in the controls and any fraud.

For information about other state initiatives, visit the website of the National Council of Nonprofit Associations (NCNA) at **http://www.ncna.org**. (Look for the page that discusses Sarbanes, and then scroll down to the bottom to find the link to the chart that describes state initiatives.) NCNA is a network of nearly 40 state and regional associations of nonprofit organizations.

At the federal level, the Senate Finance Committee opened hearings on nonprofit accountability on June 22, 2004. The Senate Finance Committee staff drafted a "Discussion Document," which included possible reforms in many different areas. Among others, the staff proposed the following changes that would involve the IRS:

- The IRS would review the tax-exempt status of public charities on every 5th anniversary of the IRS' granting of this status.
- The IRS would set new or revised standards for its annual information return, the Form 990. The goal would be to improve the return's quality and scope.
- The CEO would be required to sign a declaration that processes and procedures are in place to ensure the accuracy and completeness of the Forms 990 and 990-T. In order to sign the declaration comfortably, senior management would need to ensure that processes, procedures and controls over the Form 990 and 990T are adequate.

After the hearings and with the encouragement of the Senate Finance Committee, Independent Sector, a coalition of not-for-profit organizations, formed the Panel on the Nonprofit Sector ("panel") to make recommendations to Congress that would be designed to improve the oversight and governance of charitable organizations. The panel, comprised of 24 leaders of nonprofit and philanthropic organizations, recently issued initial recommendations for comment and expects to issue a final report in the spring. With regard to internal controls, the panel emphasized the importance of establishing a system of internal controls appropriate to the organization's size, functions, and structure. [5]

Independent Sector set up a special website at **http://www.nonprofitpanel.org** that provides more information about the panel, including the full text of the initial recommendations.

Accountability and informed awareness are consistent themes of current federal and state initiatives as well as those of the panel. All of the concerned parties are focusing on the importance to not-for-profit organizations of sound internal controls along with up to date policies and procedures that are functioning effectively throughout the institution.

Our Objectives

We believe that, notwithstanding activities at the state and federal level, this is a time when closer scrutiny of internal controls is appropriate for colleges, universities, including those with AMCs, and other not-for-profit educational institutions. Defining individual accountability for key control activities, especially in large, decentralized institutions, is increasingly important in today's environment. Stakeholders are scrutinizing institutions more closely and raising the bar on expected control behavior. Institutions of all types and sizes should be prepared to provide greater assurance to regulators, lenders, donors and other stakeholders about the effectiveness of internal controls.

This paper is designed to help directors, officers, and other senior managers of public and private research universities, including those with AMCs, as well as from smaller private colleges and other educational institutions understand the:

1. Definition of internal controls and the components of an effective system of internal controls
2. Steps that institutions should take to strengthen their internal controls—where should they begin and what should they do
3. Role of information technology (IT) controls in the current educational institution environment
4. Roles that directors, officers, internal auditors, and external auditors should play in the process of assessing and enhancing internal controls

II. What Are Internal Controls?

Internal controls mean "different things to different people," [6] which can create confusion and lead to miscommunication. The Committee of Sponsoring Organizations (COSO), which was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting known as the Treadway Commission, continues to be dedicated to enhancing the quality of financial reporting. COSO developed a common definition of internal controls that provides a standard against which all organizations can assess their controls. Internal control is defined as:

"A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations" [7]

Chart 1 on the next page provides several examples of the application of the three control objectives within the college and university environment.

Chart 1

Applying Control Objectives in the Higher Education Environment

Good Internal Controls Help To Ensure:

Effective and Efficient Operations. For example:

- A large research university has a multi-billion dollar endowment that is invested in a wide range of traditional and nontraditional investment vehicles to maximize its investment return and spread risk.
- An institution is beginning an aggressive capital campaign and will be assessing its resource requirements (e.g., people, systems) to effectively manage it.
- A university is embarking on a sizable capital construction program to renovate its student union as well as dormitories and desires to have an adequate control structure to manage this new initiative.
- An institution is implementing a new general ledger system and wants to ensure that the implementation will be within budget and that the resulting system will meet its desired business objectives.

In each of these examples, good internal controls give the stakeholders (i.e., benefactors, donors, students, parents, IT users) more faith in the institution's ability to manage its operations effectively and efficiently so that it can fulfill its missions of education, research and community service.

Reliable Financial Reports. For example:

- A state legislator uses a report that has been reconciled to a public university system's annual audited financial statement. The legislator wants to get a sense of how the institution has administered the prior year's appropriations.
- University department heads and chairs monitor financial reports each month that compare their department's budgeted expenses to their actual expenses to assess whether they are on target to meet their budget.
- The National Institutes of Health (NIH) reviews a financial status report from a research university to track its use of NIH grants and contracts.
- A lender reviews a college's annual financial statement to make sure that it is complying with the terms of its debt agreements.

In each of these examples, good internal controls give the users of financial reports (i.e., the legislator, department heads and chairs, NIH, lender) greater confidence in the reliability of the financial report.

Compliance with Laws and Regulations. For example:

- A college files its Form 990 with the IRS on a timely basis, and the tax return evidences that the institution complies with IRS rules and regulations.
- A university undergoes a self-assessment of its faculty effort reporting policies and controls to ensure it is in compliance with federal research sponsors rules and regulations.
- A trustee asks the chief financial officer (CFO) about compliance with the institution's conflict of interest policy.
- A compliance officer at a major AMC develops and monitors appropriate policies and procedures related to the Health Insurance Portability and Accountability Act (HIPAA).

In each of these examples, good internal controls give the stakeholders (e.g., IRS, federal sponsors, trustee, compliance officer) more confidence that the institution and its employees have complied with laws and regulations.

Officers and directors should assess their comfort level with the internal controls of their respective institutions in each of the three areas referred to in Chart 1.

Now that we know what internal controls are and how important they are to stakeholders, how does an institution ensure that its controls are functioning as intended? That's where the framework is important—it formalizes a set of conditions that can be commonly understood and accepted by all parties and that will foster good controls. *Internal Controls—Integrated Framework*, which was authored by PricewaterhouseCoopers for COSO and published in 1992, describes five interrelated components that are needed for internal controls to be effective:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring

The **control environment** sets the tone at the top from directors and officers. One aspect of the institution's control environment would be its written code of conduct. Other aspects are less tangible but still very important. Examples are the time and attention the board members devote to such activities as reviewing annual business risk assessments; reviewing the adequacy of the institution's policies, procedures, and controls; meeting with internal and external auditors; and evaluating the results of the annual audit.

Every institution faces risks and must find a way to manage them. Under the COSO framework, "**risk assessment** is the identification and analysis of relevant risks to achievement of the objectives." [8] Each word in that sentence is significant. First, an institution must set its strategic objectives. Ideally, the strategic objectives of the decentralized and functional units are consistent and aligned with those of the institution as a whole. Then the institution identifies the risks to achieving (or not achieving) its objectives. In the next phase, the institution estimates the significance of each risk as well as the likelihood of it occurring, and then establishes appropriate internal controls to manage the risk.

For example, if a university's strategic objective is to increase its federally sponsored research funding, then it should pay particular attention to the related compliance risks. The institution must ensure that it has adequate controls in place to ensure its compliance with research sponsors' rules and regulations and that it has in place the people, processes and systems to manage an even greater volume of sponsored projects.

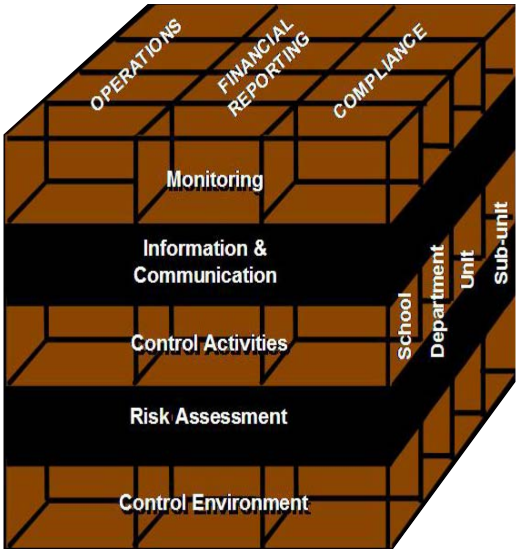
Control activities are the policies and procedures that management establishes to help ensure that its directives are carried out. Examples of control activities include ensuring that a purchase order is approved by a supervisor prior to purchasing goods, verifying that the goods have been received prior to payment, reconciling cash to bank statements on a periodic basis, properly segregating duties over liquid assets, and tracking the custody and use of fixed assets.

The right **information** must be identified, collected and communicated so that employees can carry out their responsibilities as intended. The *quality* of the information is key, that is, the information must be current, timely, accurate, accessible, and on point. **Communication** of high-quality information within the campus community is equally important. Communication tools can be as informal as one-to-one conversations and as formal as policy manuals.

If, for example, an institution wants to increase its undergraduate enrollment, then it must be able to manage an increasing number of student applications and admissions. When the new students arrive, the institution must have sufficient housing as well as the capacity to register, advise, and teach a greater number of them. In short, an institution's strategy to increase its enrollment will affect nearly every administrative and academic process. Managing and controlling the flow of information about the new strategy across the campus—and ensuring that there is clarity around the policies and processes that support and facilitate the flow of information with respect to this specific strategy—will be critical to the institution's success.

The last component concerns establishing effective monitoring controls. One example of a **monitoring control** would be a CFO's review of a report that compares budget-to-actual unrestricted and restricted revenue as well as expense activity by school over a given period. An effective monitoring control includes not only the review, but also the specific follow up inquiries that result in corrective budgetary actions.

The following cube depicts the five components of internal control—on the front of the cube—as well as the three control objectives on top of the cube.



The three objectives concern operations, financial reporting and compliance.

The five components—monitoring, information & communication, control activities, risk assessment, and control environment—must be in place in order for a control to be effective.

Several years after *Internal Control—Integrated Framework* was published, COSO asked PricewaterhouseCoopers to develop a framework to address enterprise risk management. In September 2004, COSO released *Enterprise Risk Management—Integrated Framework.* [9] Enterprise risk management (ERM) is designed to take the internal control framework a step further to satisfy an institution's need for effective internal controls *and* effective risk management. (For more information on enterprise risk management, see Appendix II.)

III. How to Enhance Internal Controls

Generally speaking, the larger and more decentralized an institution is, the more important written institutional control standards, well documented policies and procedures, and formal training and communications programs will be.

An institution's size affects how it assesses and enhances its internal controls. For example, smaller institutions, [10] such as liberal arts colleges, generally have fewer officers and staff members, making an appropriate segregation of duties more of a challenge. Although control activities are likely to be informal at smaller institutions, the direct involvement of senior management often compensates for the informality.

Other factors also determine the level of effort required to assess and enhance internal controls. One is whether or not an institution's policies and procedures are well defined and documented, and another is how centrally managed an institution is. Assessing and enhancing internal controls for an institution that is centrally managed will likely take less effort. Generally speaking, the larger and more decentralized an institution is, the more important written institutional control standards, well documented policies and procedures, and formal training and communications programs will be.

Another factor is whether an institution outsources certain functions (e.g., student loan processing, investment management, payroll) to external parties. When electing to outsource certain business functions, institutions need to consider the provider's system of internal controls as though it were their own in order to ensure that the provider addresses the appropriate risks. Also, institutions must define and execute monitoring controls over the outsource provider's activities.

In summary, such factors as the following will affect how an institution assesses and enhances its internal controls:

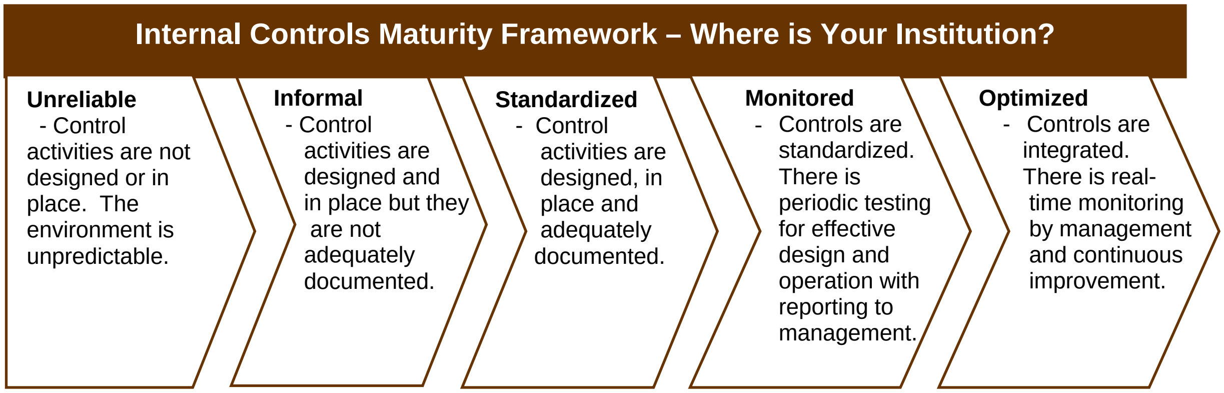
- Its size
- Extent to which it is decentralized or centralized in its business operations
- Degree to which policies and procedures are already well defined, documented, communicated and taught
- Whether it outsources any business functions to external providers

As institutions initiate actions to assess and enhance their internal controls, they should keep these five factors in mind.

Actions to Take

Where should an institution begin? **Start by assessing the controls already in place.** Every institution will fall somewhere on the Internal Controls Maturity Framework illustrated in Chart 2.

Chart 2



Internal Controls Maturity Framework – Where is Your Institution?

Unreliable - Control activities are not designed or in place. The environment is unpredictable.

Informal - Control activities are designed and in place but they are not adequately documented.

Standardized - Control activities are designed, in place and adequately documented.

Monitored - Controls are standardized. There is periodic testing for effective design and operation with reporting to management.

Optimized - Controls are integrated. There is real-time monitoring by management and continuous improvement.

Our experience shows that the internal controls of most educational institutions are likely to be "informal," the second box on the left. Institutions are likely to have control activities in place, such as required approvals and verifications, but little documentation of the controls. The controls are likely to be very "people dependent" and not standardized across the institution. This poses problems when individuals change jobs or retire and do not teach their successors their procedural control responsibilities. Formal training and communications programs as well as monitoring procedures are most likely not in place. Risk assessment and management programs also may not be in place.

The goal for most educational institutions is to start moving "rightward" along the Internal Controls Maturity Framework.

Sarbanes is requiring public companies to go from the left side of the Internal Controls Maturity Framework, from "informal," for example, to "optimized" on the right in a very short period of time. It is unrealistic to expect universities and colleges to move that far that quickly—as long as it is not required. The goal for most educational institutions is to start moving "rightward" along the Internal Controls Maturity Framework.

The following provides an example of an institution that moved “rightward” along the Internal Controls Maturity Framework in response to a problem with cash management.

Example:

A large multi-campus institution has eight transaction-intensive locations on its campuses that accept cash payments. Only one of eight locations has written procedures. The other locations rely on the knowledge of long-time employees. An internal audit shows that cash at one location is not being deposited on a regular basis. Also, the employee who makes the bank deposits also counts the cash and completes the deposit slip. A key employee at that location was on long-term sick leave, and the remaining employees did not know what to do. They were aware that controls over cash were haphazard at best, and uncomfortable about the situation. This institution developed summary written procedures for all eight locations and trained the employees to help ensure accountability in the decentralized environment.

The actions that we recommend on the following pages may seem familiar. In many respects, enhancing internal controls is very much like other campus initiatives that involve significant change. The success of all such initiatives—institutional compliance programs, for example, or major systems implementation—depends on well-known factors such as good communications.

Achieve a top-down commitment to internal control. Everyone at the top, from the audit committee to the president to the chief financial officer and internal auditor to the administrative and academic department heads, should understand and support the internal control initiative. For example, the CFO of a small centralized college assigns the project’s implementation to the controller, but he announces the controls enhancement project himself and makes its importance to him and the audit committee clear.

Perform a risk assessment in order to determine the most significant areas of vulnerability. Before enhancing internal controls, colleges and universities should identify their most critical risks, and then focus on enhancing the related controls. Enterprise risk management or ERM, which we briefly mentioned on page 9, may be a valuable new tool for colleges and universities. ERM is designed to help institutions identify potential risks (i.e., strategic, reputational, financial, compliance, and operational risks), manage them, and provide reasonable assurance regarding the achievement of the institution’s objectives. (For more information on ERM, see Appendix II.)

For more information about the risks that colleges and universities face, see PwC’s and NACUBO’s paper, ***Developing a Strategy To Manage Enterprisewide Risk in Higher Education,*** at: www.pwc.com/education.

Although financial reporting is a risk-intensive area for companies with publicly-traded stock—because investors must be able to rely on corporate financial reports for the financial markets to function properly—it is not usually the most significant risk for colleges and universities. The most significant risks for educational institutions are likely to also involve operational, strategic, compliance, and reputation issues. For example, student enrollment and tuition discounting may present significant operational and strategic risks for a tuition-dependent institution. Alternative investments may present significant operational risks for an institution with an endowment that is heavily invested in venture capital, hedge funds and other types of alternative investments.

Compliance risk is likely to be significant for most colleges and universities. They face numerous compliance risks related to federally funded programs, such as student financial aid and sponsored research as well as clinical billing practices in AMCs. As a condition of receiving federal funds for financial aid and sponsored research purposes, institutions must maintain internal controls that provide reasonable assurance of compliance with federal rules and regulations that could have a material effect on their federal programs. Independent auditors are required to obtain an understanding of an institution's internal controls over federal programs and perform tests of them in audits mandated by the Office of Management and Budget (OMB).[11]

Compliance risk is likely to be significant for most colleges and universities. They face numerous compliance risks related to federally funded programs, such as student financial aid and sponsored research as well as clinical billing practices in AMCs.

Colleges and universities have been required to undergo rigorous OMB compliance audits, including such assessments of controls over the administration of federal awards, for more than 10 years. Unless they receive federal funds, companies with publicly traded stock have not been subject to these types of audits.

It is possible that the Government Accountability Office (GAO) might impose even higher standards on recipients of federal funds in the future. The GAO establishes standards for government audits, including those mandated by OMB, and so its views are very important for institutions that receive federal funds.

The GAO's views are reflected in its December 9, 2003 comment letter to the Public Company Accounting Oversight Board (PCAOB):

> "GAO strongly believes that management's assessment of the effectiveness of internal control, along with the auditor's attestation on that assessment, are critical components of monitoring the effectiveness of an organization's risk management and accountability systems. Auditors will better serve their clients and other financial statement users and will better protect the public interest by providing assurances about the effectiveness of internal control. In this regard, GAO seeks to lead by example in establishing an appropriate level of auditor reporting on internal control for federal agencies and programs, and for entities receiving significant amounts of federal funding." [12]

Evaluate the control environment, which establishes the overall tone for the institution. One component of the control environment would be how well the institution defines individual accountability and responsibility for key control activities. Another component would be how well an institution promotes ethical values. For example, activities like those in the following box would demonstrate an institution's commitment to integrity:

For more information about codes of conduct and conflict-of-interest policies for colleges and universities, see PwC's paper, ***A Foundation for Integrity***, at: www.pwc.com/education.

Demonstrating an Institution's Commitment to Integrity

A college provides ethics training. Faculty, staff, and officers at all levels are required to complete this training.

A university has a written code of conduct. All employees are held to the same standard and disciplined equally for violations.

Managers at all levels of the institution are informed about how to solicit the ethical views of potential job candidates.

The board also helps to set the appropriate tone at the top. Evidence of good governance by the audit committee, for example, would include:

- All members of the audit committee are independent (i.e., members do not have financial interests in the organization).
- At least one audit committee member has financial expertise.
- The audit committee meets as often as is necessary with the internal and external auditors to carry out its responsibilities.
- The audit committee has a written charter that is periodically reviewed and updated. The charter summarizes members' responsibilities (see Chart 3 below).

Chart 3

Audit Committee Responsibilities [13]

The audit committee is responsible for:
All facets of the relationship with the external independent auditor, such as appointment, compensation, and retention as well as review of the audit plan, audit fieldwork, reports, and management letter, including recommendations, along with asking for the independent auditor's evaluation of management.
Oversight of financial management
Oversight of the institution's internal control structure
Reviewing financial statements and making sure that they are complete and seem reasonable based on the committee's understanding of the institution's financial health
Oversight and review of federal and state tax filings
Identifying and monitoring related party transactions
Reviewing policies for conflicts of interest, ethics, and related party disclosures
Monitoring legal matters that could affect the institution's financial health or its financial reports
Being advised regarding the adequacy of insurance coverage
Recommending improvements and remedies when problems are noted
Initiating and overseeing any special investigations that it believes are needed

Evaluate the control activities. Policies and procedures are control activities. Policies establish what should be done, and procedures are the actions that must be taken to carry out the policies. [14] Although policies, procedures, and controls are related, the guidance in the following box helps distinguish the differences among them.

Reconciling Bank Accounts

A college's **internals controls** over bank accounts provide for reconciliations and reasonableness tests as well as periodic cash counts by internal audit. The internal controls also provide for the controller to maintain a complete list of open accounts along with month-end balances and for the treasurer to review it monthly.

According to the college's **policy**, all bank accounts with average monthly balances in excess of $10,000 and/or activity averaging $50,000 or more should be reconciled monthly. Per the policy, open accounts with balances or activity levels smaller than those outlined above should be reconciled at least quarterly.

Each month a staff member reconciles the monthly bank statement within limits of 0.1% of the average balance or $50, whichever is greater. The supervisor reviews the completed reconciliations within one week, and provides evidence of his review by initialing the work. These are the **procedures**.

Control activities include transaction-level controls, such as:

- Physical controls to safeguard assets, such as keeping cash in a locked safe
- Segregation of duties, so that, for example, one person counts cash and completes the deposit slip, and another deposits the cash in the bank
- An imbedded technology edit that checks the accuracy, completeness and authorization of transactions

Internally, communication should flow *down* from management to staff, *across* from one department to another, and *up* from staff to management.

General computer controls and application controls are also examples of control activities. We provide more information about information technology controls in Section IV of this paper.

Identify and collect information that employees need to perform their jobs; develop a communications strategy to make sure the information gets to the right people. Internally, communication should flow *down* from management to staff, *across* from one department to another, and *up* from staff to management. Everyone must be clear about their roles and responsibilities, including how they relate to the work of others. Institutional policies and procedures must be widely communicated and understood.

Documentation of policies and procedures, with a specific identification of control procedures, is a best practice. We are often asked how much documentation is sufficient. It should be detailed enough that management can communicate the control throughout the institution and expect staff to understand it. It should provide answers to the following questions:

- What is the risk being controlled?
- What is the control activity?
- Why is the activity performed?
- Who (or what system) performs the control activity?
- When (how often) is the activity performed?
- What mechanism is used to perform and monitor the activity (reports and systems)?

External stakeholders, such as bond holders, lenders, donors, state and federal agencies, are becoming more interested in and aware of an institution's control environment. They want to know whether the institution effectively communicates responsibility and accountability for controls, and then whether it effectively monitors to make sure controls are working as intended.

Create workable mechanisms for monitoring compliance, reporting and operational processes to prevent or detect discrepancies and inefficiencies. It is important to monitor activities and provide for adequate follow up. If a problem is found, it must be investigated and, if indicated, corrective actions should be taken.

Monitoring has three subcomponents:

- Ongoing monitoring – Ongoing monitoring activities include regular supervisory activities that occur in the ordinary course of business.
- Periodic monitoring – Periodic monitoring activities include monthly or quarterly reviews that management performs to test the effectiveness of established procedures.
- Reporting deficiencies – There must be a process in place to report deficiencies to the appropriate level in the institution, where corrective actions can be taken.

High-level examples of monitoring controls include institutional compliance programs, internal audits, and audit committee activities. More detailed examples are presented in the box on the next page.

Three Examples of Monitoring Controls

1. Each month, the budget director reviews a report comparing expense activity by department to its budget.
2. A senior manager reviews budgeted capital construction costs for a specific project with actual costs.
3. Directors review annually a report identifying conflicts of interest for officers.

Management's responsibility is to establish effective monitoring controls. Internal audit's role should be to assess whether management's monitoring controls are functioning as intended.

Sustain the internal control enhancement program. Enhancing controls is a continuing process—very much like the institutional compliance programs that many institutions already have in place. Ongoing enhancements to internal controls help institutions proactively respond to changes involving not only regulations, but also people, processes, and technology.

Ongoing enhancements to internal controls help institutions proactively respond to changes involving not only regulations but also people, processes, and technology.

Similar to its oversight of an institutional compliance program, the effectiveness of an institution's program to enhance internal controls should be assessed annually. To ensure that the program continues to be working, the audit committee should require monitoring and periodic reporting as to the effectiveness of the institution's internal control structure.

The ongoing process to sustain and enhance internal controls should:

- Have clearly defined and documented control procedures
- Reinforce specific accountabilities at both the central and decentralized unit levels
- Include human resources mechanisms to reward the desired behaviors as part of annual performance objectives
- Be visibly supported by the institution's senior management and its audit committee
- Look for ways to streamline and simplify the processes and controls—a reduction in the number of redundant controls can lead to a more sustainable process
- Develop an adverse action policy to evaluate, report, remediate and monitor exceptions
- Communicate policy and procedure changes widely and often
- Establish training programs for employees whose roles have changed as well as for new employees

For example, the research university described in the box on the following page established training programs for employees in decentralized units who had newly assigned accountability for controls.

Example:

When a large research university assessed its controls and defined accountability campus-wide, it found that many employees who were responsible for key controls in decentralized units did not have the necessary skills to execute newly assigned control activities. Training was needed.

Note:

1. When enhancing controls, take time to assess the competency of employees in decentralized units who are being held to new, higher levels of accountability.
2. Participation of central finance administrators should be considered in the hiring of new departmental employees with financial responsibilities to make sure they have the needed skills.
3. Training for employees in decentralized units who are responsible for key controls should be ongoing.

Lessons Learned from the Corporate World

The lessons learned from the recent first round of Sarbanes-mandated internal control assessments in the corporate world have included the following:

Organization-wide

- It takes more effort to assess and test the effectiveness of internal controls than was originally estimated.
- All documentation and testing should be centralized and standardized.
- The best way to accomplish the assessment is to start by documenting and testing entity-wide monitoring controls. After that, document and assess more detailed control activities in decentralized units.
- If senior leaders are visible and close to the assessment, it will progress more smoothly.
- Preventive controls that catch errors before they occur are much more efficient than detective controls that allow errors to occur that must then be identified and corrected.

Controls are most effective when employees understand the objectives and the reasons behind the tasks they are asked to perform.

Communication

- Controls are most effective when employees understand the objectives and the reasons behind the tasks they are asked to perform.
- Good communication among decentralized units and administrative functions leads to better internal controls.
- Structured training and communication are keys to success and should be essential parts of the formal project plan.

Information Technology

- Assessing information technology (IT) controls takes time. Linking IT applications to business processes early in the project is especially important given that IT controls are usually less formal and not well evidenced.
- Maximize the use of automated IT controls to improve efficiency.
- Early identification of information systems applications allows more time to test and remediate controls.

Human Resources

- Functional unit and departmental administrators and business managers must “own” the controls. This is a key success factor. When managers take ownership of the controls they are responsible for, the controls are much more likely to be effective.
- An important part of a senior manager’s performance evaluation should be linked to how he or she advocates for strong internal controls and holds people accountable to them.

Many of these lessons would apply to the higher education environment. For example, regarding the last two bullets, in a large decentralized university, departmental administrators and business managers need to understand that they are responsible for the controls and will be held accountable for compliance with them.

IV. Information Technology Controls

Information technology (IT) controls are an integral component of an effective internal control structure. Among others, essential elements include: well-defined policies over IT security and access; adequate documentation of program changes; and skillful project management of IT systems and upgrades. One challenge is the maintenance and monitoring of controls in the decentralized, open access IT infrastructure found at most educational institutions. If IT controls are not effectively addressed, the potential for financial loss increases, but even more damaging to an educational institution can be its loss of reputation.

If IT controls are not effectively addressed, the potential for financial loss increases, but even more damaging to an educational institution can be its loss of reputation.

Protecting sensitive information, such as student records, patient records, or employees' social security numbers, is also a significant challenge. Technology officers who participated in the annual Campus Computing Survey identified network and data security as the top IT issue more often than any other single issue. [15] Many institutions—42 percent according to a *Chronicle of Higher Education* and Gartner, Inc. survey—have a security officer who focuses on campus security policies and procedures, user education, and security hardware and software. [16] According to the same survey, 9 percent of institutions that don't currently have a security officer plan to designate one in the next year.[17]

Our goal in this section is to define the nature of IT controls and provide selected examples of how they are integrated into the institution-wide control structure. We also want to raise awareness of the importance of integrating an assessment of IT controls into the broader assessment of institutional controls to manage the risk of financial loss as well as reputational damage.

Prior to assessing and implementing IT controls as part of the broader internal control framework, it is important to understand how IT controls are defined.

1. ***IT application controls*** help provide control over the data that is entered into the system, such as gifts. They help to ensure that transaction processing is accurate and complete.

2. ***IT general controls*** help to ensure the proper operation of IT systems over time. General controls include those over data center operations as well as system software acquisition, maintenance, and access security.

The categorizations above are consistent with the COSO framework. Another framework, which maps to COSO, is Control Objectives for Information Technology (CObIT). [18] COSO provides a structured definition of internal control that is built around the idea of risks to an organization meeting its objectives. CObIT is a more detailed framework for controls related to the governance, management and delivery of information technology within an organization.

IT application and general controls have not changed significantly in the last decade. However, the latest generation of technology, Enterprise Resource Planning or ERP, has shed a much brighter light on the importance of IT controls.

Specifically, ERP solutions, such as PeopleSoft, Oracle, and SAP, come with powerful inherent functionality that allows users to enhance internal controls in the IT area and help people use IT to manage risks. However, internal control functionality needs to be invoked or "configured" in the ERP system in order to work. Implementing an enterprise system does not automatically guarantee that an institution will have a strong control environment. As older systems are decommissioned and processes are reworked, the controls must change as well. They must be redesigned to fit the new environment and reviewed on an ongoing basis. If not, our experience shows us that IT controls will degrade over time.

A particular challenge for colleges, universities, and AMCs is ensuring that appropriate controls are in place for enterprise systems that are supported by departmental users. We provide examples below.

Example #1: IT Monitoring Controls – Systems Development Strategy

A highly decentralized university implements a new enterprise financial system. Central IT establishes vigorous COSO-based controls as part of the initial design of the new enterprise system. Principal investigators continue to use a legacy grants management application to track sponsored projects, and development officers continue to use a legacy gifts accounting system. The institution has identified within its systems development methodology the need to set minimum standards for internal controls over financial applications, including the grants management and gifts accounting systems.

In this example, the maintenance of the two applications rests with the sponsored research office and the development office, respectively. If the institution decides at a later date to implement sponsored research and gifts modules in addition to the financial package, then appropriate controls can be built in. In the meantime, central IT should collaborate with sponsored research and gift system users to establish minimum standards. Management might consider developing appropriate written policies and holding training sessions as well as one-on-one conversations with users to explain why the policies are important. Ideally, the departments should work with central IT to develop appropriate controls. Senior-level involvement in strategic decision making is critical to effective systems implementation. When senior-level involvement is lacking, systems implementations are more likely to be delayed or over budget or the organization might miss opportunities to take full advantage of the system's capabilities.

Senior-level involvement in strategic decision making is critical to effective systems implementation. When senior-level involvement is lacking, systems implementations are more likely to be delayed or over budget or the organization might miss opportunities to take advantage of the system's capabilities.

Example #2: IT Application Controls – Payroll Edit Check

A university converts its legacy, mainframe payroll system to a new ERP solution. The legacy system historically relied on manual controls outside the system to limit additional payments that could be made to qualified employees. The university configures an edit check within the payroll system to replace the old manual control.

In this example, the university took advantage of the new ERP system's edit control capabilities. In order to ensure all helpful edit functions were considered, management assembled a project team of interested and engaged business users who were committed to making changes, empowered with the ability to authorize changes, and responsible for owning their changes. If IT personnel alone are tasked with making all application edit control decisions, new systems rarely meet user needs.

Example #3: IT General Controls – Access Security

A university converts its legacy, mainframe financial system to a new ERP solution. The legacy system relied on manual controls outside the system to segregate users' duties. The university uses the ERP's capabilities to implement an automated security architecture to replace the old manual controls with inherently more efficient and effective automated controls.

In this example, the university made a conscious decision to take on a short-term, very labor-intensive exercise to realize more efficient, automated long-term benefits. The university documented each user's job description right down to the functional roles the user could execute in the system. This "role based" or "rule based" security effort served as the cornerstone of the university's plan to implement an overall identity management program. The program was designed to help ensure that each user's identity was automatically protected, and that unauthorized users, including hackers, were effectively excluded from the systems. Identity management is currently the number one IT controls issue being addressed by Sarbanes filers.

Where should an institution that wants to enhance its IT controls begin? Section III of this paper outlines a recommended process for enhancing internal controls. We suggest using a similar process for IT controls that starts by assessing the IT controls already in place, and then moves on through all of the steps. Consider using the CObIT framework mentioned on page 17. Also, keep in mind that enhancing IT will likely require specialized knowledge of both internal controls and IT.

V. Institutional Governance and Oversight over Internal Controls

In this section, we consider internal controls from the perspective of directors, officers, and internal and external auditors.

Directors

The *Attorney General's Guide for Charities,* which was published by the State of California in 1988, says that directors are ultimately responsible for the organization:

> "Directors may delegate many of their powers to others, such as officers and employees, but the directors are ultimately responsible for all corporate decisions." [19]

Directors set the very important "tone at the top" of the institution. They are charged with the ultimate responsibility for overseeing the institution, its officers, and staff—even though they are not on campus 24x7 making sure that everyone is behaving exactly as they should. They can be more confident that the institution is running smoothly if they know it has an effective system of internal control in place.

Directors should consider such important questions as those in Chart 4 on the next page. Taken together, all of these areas help to shape the institution's internal control environment.

For more information about leading practices for higher education audit committees, see PwC's paper, ***The Changing Role of the Audit Committee***, at: www.pwc.com/education.

Chart 4

Questions for the Board's Consideration by Area of Responsibility [20]

Strategy and Planning
Does the board bring insight, knowledge, judgment, and analytical skill to the strategic planning process?
Are directors' expertise, perspectives and judgment valued and embraced by the institution's officers?
Does the board ensure that the strategic planning process is sufficiently robust?
Risk Management
Is the board satisfied that the institution's officers have an effective risk management process in place?
Does the board ensure that the risk management program effectively aligns the strategy, objectives, risks, activities and internal controls?
Are directors comfortable that the roles and responsibilities for officers, faculty and staff—that is, everyone in the campus community—are clearly defined in the institution's risk management program and that individual accountability has been established?
Tone at the Top
Has management put into place a code of conduct and made sure that employees know about and adhere to it? Does the code include provisions about conflicts of interest?
Are directors sufficiently confident that the institution recruits people with the right values and that it reinforces desired behaviors through its human resources practices?
Is everyone in the campus community required to confirm in writing that they comply with the code of conduct? Are violations of the code taken seriously?
Measuring and Monitoring Performance; Managing Information
Does the board ensure that performance measures are linked to the institution's goals and that they measure the right things?
Do the institution's information systems provide management and the board with timely, current, and accurate information? Is it easily accessible? Is it on point?
Evaluation, Compensation and Oversight of Officers
Does the board set clear-cut and comprehensive criteria, metrics and qualitative measures to evaluate the president's performance as well as that of other key senior officers, such as the chief financial officer?
Does the board ensure that compensation decisions for senior officers are formulated by truly independent directors?
Does the board continually monitor performance and provide constructive feedback?
Is the board's oversight of officers appropriate? For example, does the board provide the right level of oversight to financial officers who are responsible for establishing and maintaining internal controls?
Financial Reporting, Tax Reporting and Transparency
Does the board understand and embrace its responsibilities for financial and tax reporting?
Is the board comfortable that the financial reports are sufficiently transparent?
Board Dynamics
Do individual directors have the requisite skills, integrity, industry knowledge, interpersonal and other qualities that enable the board as a whole to function effectively?
Is the board small enough to act cohesively and large enough to bring the needed knowledge and skills to the job?
Do board members meet often enough to fulfill their responsibilities and are they prepared for meetings?
Does the board regularly evaluate its performance?

Officers

In general, officers are responsible for managing operations while directors are responsible for providing oversight. Officers develop strategic and operational plans as well as internal control, risk management, and ethics programs while directors oversee them. Officers prepare financial reports, while directors, particularly audit committee members, oversee their development and review them.

Chart 5 summarizes officer's responsibilities related to internal controls, according to Sarbanes.

Chart 5

A Summary of Officer's Responsibilities per Sarbanes [21]

Officer Responsibility	Responsibilities Related to Internal Controls (Sarbanes Section)
✓	Establishes and maintains internal controls such that they are effective (Section 302)
✓	Discloses significant deficiencies in the design or operation of internal controls to directors and the institution's independent auditor; discloses identified material weaknesses to auditor (Section 302)
✓	Discloses instances of known fraud to directors and the institution's independent auditor (Section 302)
✓	Discloses whether institution has adopted a code of ethics for senior financial Officers (Section 406)

If it does not have a code of ethics for senior financial officers, we believe the institution should develop one under the board's oversight. Furthermore, consideration should be given to establishing a code of ethics for all levels of the campus community.

We have excluded from Chart 5 the requirement in Section 404 of Sarbanes that officers assess, test, report on, and certify to internal controls, since the Act does not apply to colleges, universities and other not-for-profit educational institutions. Increasingly, however, CFOs of such institutions are being asked to certify the internal controls without formal assessment, testing, and reporting. Some CFOs are, in turn, asking their subordinates and other departmental heads to subcertify.

We advise considering the underlying issues raised by the following five questions before requiring certifications or subcertifications:

1. What specifically would the CFO or his subordinates certify?
2. If the controls depend on managers in decentralized units, do they have a deep enough understanding of the controls as well as the right skill set to make the certification meaningful?
3. How broad should a subcertification from a decentralized unit be? For example, should the subcertification cover financial information or business practices or both?
4. Many key processes involve multiple handoffs of data to various departments. Can certification be meaningful without an equal level of subcertification from each department involved in the process?
5. Some key control processes involve individuals outside the campus community. Can certifications be relied upon when information and activities are the responsibilities of outside parties (e.g., alumni, joint venture partners)?

Notwithstanding the questions that should be addressed prior to initiating an institution-wide certification process, we believe that requiring a certification of controls may be appropriate at the departmental, school, or other functional unit level. For example, an administrator in the engineering department might certify that he or she has informed the central finance unit of the total amount of funds that the engineering dean has solicited for a specific purpose. Over time, as the decentralized units gain the needed skills, the certification can expand to include financial information and business practices as well as controls.

Certification can be a good way to raise awareness about accountability and the importance of sound controls. However, certification is much more complicated than it might first appear, especially for highly decentralized institutions.

Certification can be a good way to raise awareness about accountability and the importance of sound controls. However, certification is much more complicated than it might first appear, especially for highly decentralized institutions.

Internal and External Auditors

Establishing internal controls is not the primary responsibility of the internal or external auditor but both play important roles. According to the Institute of Internal Auditors (IIA), when directors, officers, external and internal auditors "work together well with healthy interdependence, internal controls are strong, reporting is accurate, ethics are maintained, oversight is effective, risks are mitigated, and investments are protected." [22]

One of the most fundamental responsibilities of internal auditors has been providing assurance that internal controls are in place and they are working as intended. The Association of College and University Auditors (ACUA) is a membership organization for internal auditors who work in the higher education sector. In cooperation with IIA, ACUA is working to expand the role of internal audit. According to ACUA, the traditional role of internal audit has been to evaluate:

- Information—is it reliable?
- Compliance—are employees complying with the institution's policies and procedures as well as with external laws and regulations?
- Assets—are they safeguarded?
- Resources—are they being used efficiently and effectively?
- Goals and objectives—are they being accomplished? [23]

Now internal audit's role also includes the following responsibilities, all of which are very relevant to the topics addressed in this paper:

- Internal control—internal audit should participate in activities designed to improve internal controls.
- Strategic risks—internal audit should help officers identify and assess strategic risks.
- Accountability and training—internal audit can help bring these tools to colleges and universities.
- Risk assessments—internal audit can assist individuals who perform operational and financial activities with risk assessment and management.
- Ethics—internal audit can provide training and other resources to help address ethical issues.
- Process improvement—internal audit can participate in process improvement initiatives.
- Directors—internal audit can help directors, particularly audit committee members, carry out their fiduciary responsibilities. [24]

In the corporate Sarbanes environment, the IIA has said that management should not delegate its responsibility for assessing internal controls to the internal auditor. However, internal audit can support management. PwC's Michael Barone, who directs the Firm's higher education internal audit practice, said in an article in ACUA's *College & University Auditor*: "Internal audit can play a key role in any Sarbanes-related initiative—from gap analysis to advising management and the board to documenting controls or testing controls." [25]

External auditors have specific responsibilities for evaluating internal controls under generally accepted auditing standards. In financial statement audits, they are required to obtain an understanding of the internal controls so that they can plan the nature, timing and extent of their audit procedures. Further, in federal and state compliance audits (i.e., audits of federal programs under OMB Circular A-133—see end note 11), external auditors must obtain an understanding of and test internal controls over financial reporting and compliance with the applicable regulations. In both financial statement and compliance audits, auditors must report conditions that they view as significant deficiencies in the design or operation of the institution's internal controls. Such deficiencies might affect the institution's ability to accurately prepare financial information, its ability to receive an unqualified audit report, and/or participate in federal and state sponsored programs.

Under current professional standards, the external auditor of a non-profit educational institution is required to communicate internal control deficiencies, known as "reportable conditions," that are noted during the audit to management as well as to the governing body of the institution, usually the audit committee. Auditors use their professional judgment and perspective gained by working in the higher education industry to determine the severity of the internal control deficiency. Generally accepted auditing standards define reportable conditions as "matters coming to the auditor's attention that, in his judgment, should be communicated to the audit committee because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the organization's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements." [26]

The auditor's professional standards further explain that when a reportable condition is of such a magnitude that it presents a higher level of risk to the organization, it is referred to as a "material weakness." A material weakness is "a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions." [27] Material weaknesses must be brought to the institution's attention in writing.

Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit*, established the auditor's responsibility for detecting fraud during the audit of an institution's financial statements. In this context, fraud is misstatements from fraudulent financial reporting as well as misstatements from misappropriation of assets. [28] Fraud is closely related to any discussion of internal controls because it often occurs when controls fail or when employees collude to override controls.

Under generally accepted auditing standards, the audit team must discuss the risk of fraud at an institution and what audit procedures might allow it to be detected. The auditors are not required to specifically audit with the intention to detect fraud. However, auditors are required to consider that fraud may be occurring and to design their tests with this consideration in mind. If auditors discover that a material fraud has occurred, they must bring it to the attention of the appropriate level of management (someone at a level above the perpetrator), and/or the governing board.

Finally, external auditors should provide to governing boards, usually to audit committees, and senior management their professional insight, opinion and guidance regarding what they believe are the greatest risks to the institution from a strategic, operational, financial, compliance and reputation perspective. In addition, the external auditor should provide comments and recommendations on how to prioritize steps to address key risks, and to help in providing solutions to mitigate the impact of such risks through the development (or refinement) of internal controls.

VI. Conclusion

Colleges and universities, including AMCs, as well as other not-for-profit educational institutions establish internal controls to provide reasonable assurance that they will be in compliance with applicable laws and regulations; their operations will be effective and efficient; and stakeholders will be able to rely on their financial reports. They are increasingly important in times—like now—when greater accountability is required of public and private institutions.

Internal controls are receiving more attention in the press as well as at the state and federal levels. New York and Massachusetts might consider legislation this year that would include internal control provisions. The federal government might impose higher internal control standards on recipients of federal funds in the future. Also, the Panel on the Nonprofit Sector expects to make recommendations to Congress later this year that might relate to internal controls.

We believe that college and university officers and directors who take on the challenge of enhancing their internal controls will be better able to more effectively demonstrate their commitment to a stronger control environment to their stakeholders. The chart below summarizes the actions we have recommended in this paper. Keep in mind that one size does not fit all when assessing and enhancing internal controls. Each institution has unique characteristics and needs. In general, however, taking the recommended actions should lead to better, more effective internal controls. In this era of heightened scrutiny, the question is when, not if, stakeholders will make inquiries.

Chart 6

Enhancing Internal Controls

What Is Needed	What To Do
Assessment	Assess the current state of the institution's controls using the Internal Controls Maturity Framework in Section III of this paper. Include IT controls in the assessment.
Commitment	Make a commitment to having strong internal controls. Directors and officers must set the appropriate "tone at the top" if they want to enhance the institution's controls.
Risk Assessment	Identify the institution's most significant risks. Consider reputational risk as well as compliance, operational, financial, and strategic risks. Focus on establishing controls to mitigate the risks in the most vulnerable areas.
Control Environment	Determine how the institution defines individual accountability and responsibility for key control activities at every level, including directors, officers, internal auditors, departmental administrators and business managers. Make sure that messages are clear and noncontradictory.
Control Activities	Evaluate the institution's control activities, such as its policies and procedures.
Information and Communications	Identify information needs, and develop a communications strategy to get the right information into the hands of the employees who need it to carry out their responsibilities. For example, institutional policies must be widely communicated and understood. Individual accountability must be clearly defined.
Monitoring	Establish follow-up procedures, such as staff supervision, to make sure that controls are working as intended. Other examples of monitoring controls are activities of institutional compliance programs and audit committees as well as effective internal and external audit programs.
Sustainability	Reinforce accountability by clearly establishing roles, responsibilities and accountability at all levels. Include mechanisms to reward desired behaviors. Develop ongoing training programs that enhance employees' ability to execute their responsibilities for key controls. Continue to look for ways to streamline, simplify, and enhance processes and controls.

Appendix I: The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (“Sarbanes”) was signed into law on July 30, 2002. It established new standards for corporate accountability. The U.S. Securities and Exchange Commission (SEC) is responsible for prescribing rules that implement Sarbanes.

Sarbanes includes 11 titles, as shown in the following table.

The Sarbanes-Oxley Act – Titles and Sections

Title	Section
I. Public Company Accounting Oversight Board	101 Establishment; administrative provisions 102 Registration with the Board 103 Auditing, quality control and independence standards and rules 104 Inspections of registered public accounting firms 105 Investigations and disciplinary proceedings 106 Foreign public accounting firms 107 Commission oversight of the Board 108 Accounting standards 109 Funding
II. Auditor Independence	201 Services outside the scope of practice of auditors 202 Pre-approval requirements 203 Audit partner rotation 204 Auditor reports to audit committees 205 Conforming amendments 206 Conflicts of interest 207 Study of mandatory rotation of registered public accounting firms 208 Commission authority 209 Considerations by appropriate State regulatory authorities
III. Corporate Responsibility	301 Public company audit committees 302 Corporate responsibility for financial reports 303 Improper influence on conduct of audits 304 Forfeiture of certain bonuses and profits 305 Officer and director bars and penalties 306 Insider trades during pension fund blackout periods 307 Rules of professional responsibility for attorneys 308 Fair funds for investors
IV. Enhanced Financial Disclosures	401 Disclosures in periodic reports 402 Enhanced conflict of interest provisions 403 Disclosures of transactions involving management and principal stockholders 404 Management assessment of internal controls 405 Exemption 406 Code of ethics for senior financial officers 407 Disclosure of audit committee financial expert 408 Enhanced review of periodic disclosures by issuers 409 Real time issuer disclosures
V. Analyst Conflicts of Interest	501 Treatment of security analysts by registered securities associations and national security exchanges
VI. Commission Resources and Authority	601 Authorization of appropriations 602 Appearance and practice before the Commission 603 Federal court authority to impose penny stock bars 604 Qualifications of associated persons of brokers and dealers
VII. Studies and Reports	701 GAO study and report regarding consolidation of public accounting firms 702 Commission study and report regarding credit rating agencies 703 Study and report on violators and violations 704 Study of enforcement actions

	705 Study of investment banks
VIII. Corporate and Criminal Fraud Accountability	801 Short title 802 Criminal penalties for altering documents 803 Debts nondischargeable if incurred in violation of securities fraud laws 804 Statute of limitations for securities fraud 805 Review of Federal sentencing guidelines for obstruction of justice and extensive criminal fraud 806 Protection for employees of publicly traded companies who provide evidence of fraud 807 Criminal penalties for defrauding shareholders of publicly traded companies
IX. White Collar Crime Penalty	901 Short title 902 Attempts and conspiracies to commit criminal fraud offenses 903 Criminal penalties for mail and wire fraud 904 Criminal penalties for violations of the Employee Retirement Income Security Act of 1974 905 Amendment to sentencing guidelines relating to certain white-collar offenses 906 Corporate responsibility for financial reports
X. Corporate Tax Returns	1001 Sense of the Senate regarding the signing of corporate tax returns by chief executive officers
XI. Corporate Fraud and Accountability	1101 Short title 1102 Tampering with a record or otherwise impeding an official proceeding 1103 Temporary freeze authority for the Securities and Exchange Commission 1104 Amendment to the Federal Sentencing Guidelines 1105 Authority of the Commission to prohibit persons from serving as officers or directors 1106 Increased criminal penalties under Securities Exchange Act of 1934 1107 Retaliation against informants

Most of Sarbanes' provisions are not required for not-for-profit organizations, although some (e.g., those pertaining to the audit committee) are viewed as "leading practices." Not-for-profit organizations, including colleges, universities, and other not-for-profit educational institutions, might want to consider implementing them voluntarily to improve their business processes and perception with directors, donors, grantor agencies, bond holders, students, faculty, and taxpayers. In addition, Sarbanes may prompt future federal and state laws governing not-for-profit organizations.

Two provisions in Sarbanes are applicable to not-for-profit organizations, including colleges and universities. They are Section 802 and Section 1107. Section 802, "Criminal Penalties for Altering Documents," says that organizations that destroy documents to obstruct a federal investigation shall be fined or imprisoned or both. Section 1107, "Retaliation against Informants," provides protection for whistleblowers.

The Key Internal Controls Provisions of Sarbanes

Two sections of Sarbanes—302 and 404—are particularly relevant to this paper because they deal with internal controls.

Section 302

Sarbanes' Section 302 says that officers are responsible for an organization's internal controls. Officers must certify that the internal controls are effective and they must disclose significant deficiencies in the internal controls to the audit committee and the independent auditor. They must disclose material weaknesses to the auditor. We provide the following excerpt from Sarbanes' Section 302:

> "SEC. 302. Corporate Responsibility for Financial Reports
>
> (a) Regulations Required.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m,78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

> (1) the signing officer has reviewed the report;
> (2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
> (3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
> (4) the signing officers—
>
>> (A) are responsible for establishing and maintaining internal controls;
>> (B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
>> (C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
>> (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;
>
> (5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—
>
>> (A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
>> (B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and
>
> (6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses." [29]

Section 404

Section 404 deals with management's assessment of internal controls. The assessment goes hand in hand with the certification required by Section 302. Management needs to assess the internal control environment in order to certify to its effectiveness. The following excerpt is taken directly from Sarbanes:

> "SEC. 404. Management Assessment of Internal Controls
>
> (a) Rules Required.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
>
>> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
>
> (b) Internal Control Evaluation and Reporting.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement." [30]

Under Sarbanes, management is responsible for assessing the effectiveness of internal control as of the end of the fiscal year, using suitable criteria, and documenting and reporting on the assessment.

The SEC's Role

The SEC is a federal commission charged with protecting investors and maintaining the integrity of the securities markets. Sarbanes directs the SEC to provide implementation guidance for "registrants" (i.e., companies that are registered with the SEC to publicly trade securities). In its Final Rule No. 33-8238, which was issued in June 2003, the SEC defined internal control over financial reporting as:

> "A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:
>
> (1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
>
> (2) 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 authorizations of management and directors of the registrant; and
>
> (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements." [31]

For More Information

PricewaterhouseCoopers has posted the full text of Sarbanes—along with analysis and commentary—on its website at **http://www.pwc.com/sarbanesoxley**. Interested readers may want to investigate this site for more information about Sarbanes.

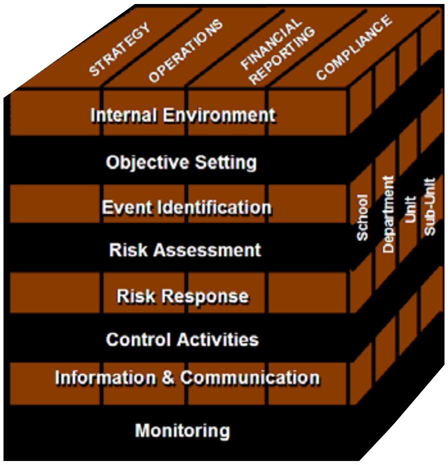
Appendix II: Enterprise Risk Management

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission published *Enterprise Risk Management—Integrated Framework* [32] in September 2004. PricewaterhouseCoopers is its author.

Enterprise Risk Management—Integrated Framework expands on *Internal Control—Integrated Framework,* which was issued in 1992. It does not replace it. The new enterprise risk management framework is designed to satisfy an organization's need for effective internal controls *and* effective risk management. According to Frequently Asked Questions on COSO's website at **http://www.coso.org**:

> "The frameworks are compatible and are based on the same conceptual foundation. We believe the consistent conceptual underpinnings are a major strength of the two models."

The following cube depicts the enterprise risk management framework.



In the ERM framework, an organization's objectives are categorized as shown on top of the cube as:

1. Strategy
2. Operations
3. Reporting
4. Compliance

The framework has eight components as shown on the front of the cube. ERM considers activities at all organizational levels.

COSO defines enterprise risk management as follows:

> "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." [33]

The ERM framework has eight components:

1. The **internal environment** relates to the organization's culture, its ethical values, the environment in which it operates, and its risk "appetite."
2. **Objective setting** concerns the process that management uses to sets its objectives. The objectives should align with the organization's mission and be consistent with its risk appetite.
3. An organization sets its objectives, but they are affected by internal and external events (i.e., **event identification**). Events present opportunities and risks that affect the organization's achievement of its objectives.
4. **Risk assessment** is a key component. Organizations must identify risks, assess them, and find ways to manage them.
5. Management responds to risks (i.e., **risk response**). It might decide to accept them, avoid them, and/or find ways to manage them.
6. **Control activities** are the policies and procedures that the organization establishes to help make sure that it responds to risks as intended.
7. **Information and communication** concerns the way that the right information is identified and then communicated to the people in the organization who need it. Communication must flow down, across and up the organization for it to be effective.
8. The risk management process must be **monitored** through ongoing activities or periodically or both, and corrective actions should be taken when necessary.

Everyone in an organization is responsible for risk management. Directors are responsible for oversight, while officers are responsible for making it happen. The chief executive officer (CEO) usually owns the process, but other officers must support the CEO in this endeavor, manage the risks they are responsible for, and promote risk management within their departments and units.

For More Information

For more information about risk management, visit COSO's website at **http://www.coso.org**. The executive summary of *Enterprise Risk Management—Integrated Framework* is available at no charge on COSO's website.

Applicability of Enterprise Risk Management to Higher Education

Several years ago, PricewaterhouseCoopers' Education & Nonprofit practice leaders, along with NACUBO, conducted a forum of college and university business officers and other thought leaders to discuss risk management. We discussed many of the concepts that are now presented in *Enterprise Risk Management—Integrated Framework*. After the forum, PricewaterhouseCoopers and NACUBO published a paper, *Developing a Strategy To Manage Enterprisewide Risk in Higher Education.* It can be found on our website at: **http://www.pwc.com/education**. We plan to update this paper now that *Enterprise Risk Management—Integrated Framework* has been published.

End Notes

[1] For more information on Sarbanes, see Appendix I of this paper.

[2] *Internal Controls and Financial Accountability for Not-for-Profit Boards*, published by Attorney General of New York Eliot Spitzer, page 2. This booklet is available at: **http://www.oag.state.ny.us**. Click on "Charities."

[3] From a review of the legislation as well as from correspondence with the California AG's office. More information about the California legislation can be found in a brochure published by the AG's office at: **http://www.ag.ca.gov/charities/index.htm** Click on "Publications" and then scroll down to "Summary of New Law: Nonprofit Integrity Law of 2004."

[4] From the website of the Iowa Nonprofit Resource Center at the University of Iowa, which includes a summary of the law as well as the legislation. The summary was found at: **http://nonprofit.law.uiowa.edu/** Click on "Updates" and then "News." On the right hand navigator, click on "Revised Nonprofit Corporation Act (S 2274)" and finally click on the link to the summary.

[5] At **http://www.nonprofitpanel.org**, look for the Work Group's recommendations. In the recommendations, the quote can be found at: "Issue #6 DRAFT—Page 5 of 5."

[6] *Internal Control—Integrated Framework* by COSO, July 1994 edition, page 3. (For more information about COSO, see its website at **http://www.coso.org**. The history of COSO can be found in the introduction of COSO's *Report of the National Commission on Fraudulent Financial Reporting*.)

[7] Ibid, page 3.

[8] Ibid, page 4.

[9] The Executive Summary of *Enterprise Risk Management—Integrated Framework* is available on COSO's website at **http://www.coso.org**. The full report is available from the AICPA (at **www.cpa2biz.com**) in two volumes. The first volume includes the Executive Summary, as it has been posted on COSO's website, and the more detailed *Framework*. The second volume, *Application Techniques*, provides implementation guidance.

[10] Smaller institutions are usually more tuition dependent and more centralized. They may have fewer research activities and less revenues.

[11] The Office of Management and Budget (OMB) issued its Circular A-133, *Audits of Institutions of Higher Education and Other Non-Profit Organizations*, in 1990. Its name was subsequently changed to *Audits of States, Local Governments, and Non-Profit Organizations*. Circular A-133 describes the responsibilities of non-federal recipients of federal funds to manage federal assistance programs, including federally funded research and federally funded student financial aid programs. This Circular also includes the auditor's responsibilities for auditing federally funded programs. You will find the circular at: **http://www.whitehouse.gov/omb**. See also brief discussion of "Internal Control" on page 1-6 of OMB's March 2004 Compliance Supplement on the same website.

[12] From GAO 12/9/03 comment letter to the PCAOB on proposed auditing standard, *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. Comment letter can be found at: **http://www.gao.gov**. Search for key words "comment letters."

[13]*Internal Controls and Financial Accountability for Not-for-Profit Boards*, published by Attorney General (of New York) Eliot Spitzer, pages 7-10. This booklet is available at: **http://www.oag.state.ny.us**. Click on "Charities."

[14] *Internal Control—Integrated Framework*, page 51.

[15] "Technology: Keeping Networks Safe Is Administrators' Dominant Worry," by Andrea L. Foster, *Chronicle of Higher Education*, Special Report, January 7, 2005.

[16] "Colleges Face Rising Costs for Computer Security," by Andrea L. Foster, *Chronicle of Higher Education*, December 17, 2004.

[17] Ibid

[18] For more information on CObIT, see: **http://www.isaca.org**.

[19] *Attorney General's Guide for Charities*, published by the state of California, 1988, page 17. It can be found at: **http://www.ag.ca.gov/charities/index.htm**. Click on "Publications"

[20] Adapted from *Corporate Governance and the Board—What Works Best*, by PricewaterhouseCoopers, published by The Institute of Internal Auditors Research Foundation, 2000. This book is available at **http://www.theiia.org**. We selected key points from "Appendix A—Self-Assessment Guide" as well as from other sections. The full Self-Assessment Guide is a useful tool for boards.

[21] Based on the full text of the Sarbanes-Oxley Act of 2002 at **http://www.pwc.com/sarbanesoxley**. We looked for responsibilities of officers related to internal controls and ethics to develop this chart.

[22] Website of the Institute of Internal Auditors (IIA) at **http://www.theiia.org**. Click on "The IIA" on the top navigation bar. Then click on "About the Profession" and then "All in a Day's Work."

[23] Association of College and University Auditors (ACUA), Position Paper, *The Importance of Retaining the Internal Auditing Activity In-House*, at **http://www.acua.org**.

[24] Ibid

[25] Barone, Michael, “The Implications of Sarbanes-Oxley for Internal Auditors,” *College & University Auditor*, Volume 47, Number 3, winter 2003, page 10.

[26] From 325.02 of U.S. Auditing Standards (AU) 325, *Communication of Internal Control Related Matters Noted in an Audit*, published by the AICPA in June 2003.

[27] Ibid, 325.15.

[28] SAS 99 says in paragraph 6: “Misstatements arising from fraudulent financial reporting are intentional misstatements or omissions of amounts or disclosures in financial statements designed to deceive financial statement users where the effect causes the financial statements not to be presented, in all material respects, in conformity with generally accepted accounting principles (GAAP)…Misstatements arising from misappropriation of assets (sometimes referred to as theft or defalcation) involve the theft of an entity’s assets where the effect of the theft causes the financial statements not to be presented, in all material respects, in conformity with GAAP.”

[29] From Sarbanes-Oxley Act of 2002 at **http://www.pwc.com/sarbanesoxley**.

[30] From Sarbanes-Oxley Act of 2002 at **http://www.pwc.com/sarbanesoxley**.

[31] SEC Final Rule No. 33-8238 at **http://www.sec.gov**. Search for Final Rule 33-8238.

[32] The Executive Summary of *Enterprise Risk Management—Integrated Framework* is available on COSO’s website at **http://www.coso.org**. The full report is available from the AICPA (at **www.cpa2biz.com**) in two volumes. The first volume includes the Executive Summary, as it has been posted on COSO’s website, and the more detailed *Framework*. The second volume, *Application Techniques*, provides implementation guidance.

[33] From page 2 of the Executive Summary, *Enterprise Risk Management—Integrated Framework,* published by COSO in 2004 and available at COSO’s website at **http://www.coso.org**.