Achieving goals, protecting reputation*

Enterprise risk management
for educational institutions

*connectedthinking

PricewaterhouseCoopers

Contents

Could it happen here?

All too often colleges, universities, academic medical centers and other educational institutions are featured in headlines for all the wrong reasons. Whether these headlines are about strategies that have gone awry, compliance failures, financial losses or misconduct, this type of publicity is embarrassing as well as potentially damaging to an institution's reputation.

Although these headlines originate from a wide array of unfortunate events, some commonalities to consider are:

- They keep institutional leaders and major stakeholders up at night.
- While you wouldn't wish them on your toughest competitor, you can't help but think: "Better them than us."
- Your next thought is: "Could it happen here?"

We believe that the chances of unfortunate events occurring on your campus can be significantly reduced when an enterprise risk management ("ERM") process is in place and operating effectively. What is ERM? While this paper will delve into the theory and the practical details of how to begin to implement an effective ERM program, we believe the following to be the key concepts:

- ERM recognizes that because each institution of higher education engages in a countless array of activities and it pursues a wide range of objectives, it faces a myriad of risks—any one of which could be the basis for tomorrow's headline.
- ERM embodies a mindset that the risk population is too broad and too deep to be fully understood and managed solely from the leadership suite.
- ERM embraces the concept that most risks—and the degree of vulnerability a particular institution has to them today—are understood and appreciated somewhere among its rank and file employees.
- ERM is built on the cornerstone of empowering information that flows up, down and across the institution as a primary means of managing risk.
- ERM recognizes that risks cannot be avoided, but the vast majority of surprises can be minimized.
- Effective leaders understand that ERM must be continuous and dynamic because the institution's activities and objectives, and therefore its risks, are ever-changing.

Our objectives

We believe that a broader awareness of risk and risk management techniques is warranted for colleges, universities, academic medical centers, and other not-for-profit educational institutions. In all institutions, not just the largest and most decentralized, identifying risks in a framework that leads to managing them is essential as stakeholders continue to raise the bar on expected behavior and headline writers continue to focus on industry "troubles."

This paper is designed to help presidents, officers, senior management, and board members understand:

- Risk factors for not-for-profit educational institutions
- A working definition of ERM and its applicability to not-for-profit educational institutions
- The importance and benefits of ERM
- Practical steps that institutions can take to implement ERM strategies

What is
enterprise risk management?

The Committee of Sponsoring Organizations, known as COSO, defines ERM as:

"… 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,[1] to provide reasonable assurance regarding the achievement of entity objectives."[2]

ERM focuses on an institution's achievement of its objectives in the following four areas:

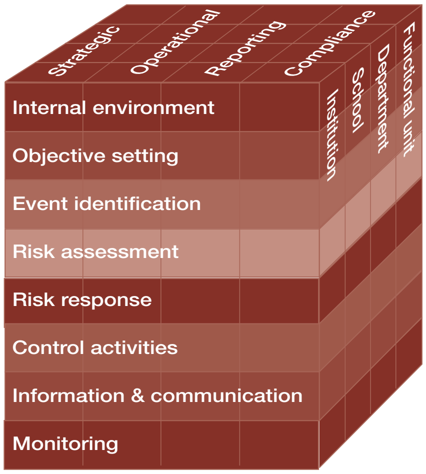
1. Strategic: High-level goals, aligned with and supporting the mission of the institution
2. Operational: Effective and efficient use of the institution's resources
3. Reporting: Reliability of the institution's external and internal reporting
4. Compliance: The institution's compliance with applicable laws and regulations

COSO recognized the need for a broadly accepted risk management framework similar to its earlier *Internal Controls—Integrated Framework*. In 2004, COSO released its *Enterprise Risk Management—Integrated Framework*, which was authored by PricewaterhouseCoopers LLP (PwC). The enterprise risk management ("ERM") framework is fully aligned with COSO's *Internal Control—Integrated Framework*, thus enabling institutions to build on their investments in internal controls as they make improvements in risk management.

The cube in Figure 1 depicts the ERM framework,[3] which consists of the four objectives noted above and eight interrelated components. Each of the eight components cuts across the four objectives. For example, there are strategic, operational, reporting, and compliance aspects of the "internal environment."

The third dimension of the cube (i.e., institution, school, department and functional unit) illustrates that each of the eight components should be assessed within various levels of the institution. For example, the internal environment of each business unit should be considered from strategic, operational, reporting, and compliance perspectives in view of the fact that there are objectives—actions that leadership wants to take—in each of those dimensions.

Figure 1:
ERM framework[3]



The eight interrelated components

1. Internal environment

The internal environment is the basis for all the other components and relates to the institution's culture, its ethical values, the environment in which it operates and its risk appetite. The environment includes the code of conduct, senior management's statements and actions concerning the importance of appropriate ethics and conduct, and the degree to which the board and officers focus on how undesirable actions are penalized and desirable conduct is rewarded.

2. Objective setting

Objective setting is the process that management uses to set its goals. The objectives should align with the institution's mission and be consistent with its risk appetite. These objectives can be strategic in nature, or they may relate to operations, reporting and/or compliance. Examples could include adopting a strategy to increase the level of federal research funding, implementing a plan to better target financial aid awards, and improving compliance with hazardous waste disposal regulations.

3. Event identification

Event identification involves recognizing and cataloguing reasonably possible internal and external events that could affect the institution's ability to achieve its objectives. For example, the strategy to grow federal research funding could be impacted by such events as a shrinkage in the availability of funds from a federal agency, the adoption of a similar strategy by a key competitor, failure to secure government approval of a critical investigational protocol, and regional economic factors that make it more difficult to attract talented researchers to a campus.

4. Risk assessment

Institutions must assess the risks that have been identified to assure that their risk management plan is properly prioritized. One of the most common techniques is to evaluate each risk from two dimensions: 1) the likelihood of the risk event taking place, as well as 2) the impact on the institution if the negative outcome of the event is not effectively reduced or mitigated. There are numerous ways to perform such assessments (see Section III below) but it is important both to apply criteria consistently and to evaluate likelihood after considering controls and safeguards that are already in place.

5. Risk response

Risk response relates to how management maps out a plan for reacting to the risks the institution faces. Responses should be consistent with their related assessment (i.e., focus initial energies on the top priority risk events, which include those with both high likelihood of taking place and high impact when they do). Planned responses must also embrace events that may have a small likelihood of happening, but near catastrophic impact if they do. One of the lessons of the hurricane season of 2005 is that institutions with more detailed business continuity plans were better positioned to resume their activities than those that did not.

6. Control activities

Control activities are the policies and procedures that an institution establishes to help make sure that it responds to risks as intended. From a risk management perspective, new control activities may involve identifying and monitoring key indicators to assure that progress toward achieving higher risk mitigation plans remain on track. Control activities should be integrated with risk responses. For example, if a key part of the business continuity plan is to have an off-campus “hot site,” a related control activity would be to periodically test the availability and compatibility of the chosen site. In the area of compliance risks, new or enhanced control activities often comprise the major risk response. For example, additional reviews of charges to sponsored research funds could be an appropriate response to the risk that inappropriate expenditures may be charged to such funds.

7. Information and communication

Information and communication concern the way that the right information is identified and then communicated to the people in the institution who need it. Communication must flow down, across and up the institution in order to be effective. Key communications around an ERM implementation would focus on the importance of the initiative, the fact that it is endorsed at the highest levels of executive management and the Board, and that each individual has a role to play in identifying and managing risks. To be effective, risk management processes must be made transparent across the institution so that those who have the ability to sense whether key initiatives are on track or in trouble—and these people often work at all levels across campus—are aware of the value of their observations and know what to do with the information they gather.

8. Monitoring

The risk management process must be monitored through ongoing activities as well as periodically. Corrective actions should be taken when necessary. The ERM process should have built-in mechanisms to evaluate the effectiveness of the decisions that it produces. A likely periodic monitoring technique would be a review by internal audit and/or institutional compliance function of the procedures management has put into place to manage and control risk, as well obtaining, as available, comparisons to results in other institutions and emerging leading practices.

Why should you be concerned about risk now?

We believe that the following reasons make a compelling case for embracing ERM sooner rather than later:

- In view of the complexity of the operating environment at a college, university or academic medical center, stakeholder interests are more effectively protected when ERM practices are being employed.
- Board members want to fulfill their obligations to assure greater accountability, and risk management is a useful tool for achieving this goal.
- ERM can help an institution prepare for the possibility of charitable reform legislation at the national or state level.
- Responding successfully to new standards issued by the American Institute of Certified Public Accountants (AICPA) may require a greater emphasis on risk management.

Operating complexity

The diversity of their operations and the breadth of their compliance responsibilities mean that institutions of higher education face some formidable challenges, including, but not limited to:

- Operating a wide array of diverse business activities in a decentralized environment
- Directing sponsored research programs
- Managing endowments, including alternative investments
- Raising private gifts and grants and abiding by donor wishes
- Controlling capital construction programs
- Educating students in an age of increasing information access
- Operating athletic programs while facing dual pressures of compliance complexity and the need to win to justify resources expended
- Maintaining information systems security, privacy and resiliency
- Complying with evolving, complex regulatory and tax requirements
- Managing international programs and initiatives

How can management deal with the initiatives related to these challenges? ERM is a management tool that can unite many seemingly separate initiatives under a common umbrella. Internal controls, compliance programs, IT implementations—all can be linked under the risk management umbrella. ERM adds value to an institution by giving management a tool for dealing with events in a way that reduces the likelihood of negative outcomes. It can:

- Quickly identify emerging risks and problem areas before they escalate and cause serious harm
- Reduce response time for new or changing risks
- Focus efforts on the most important issues and concerns and direct both financial and human capital to the right places and the highest risk areas

Expanded board accountabilities

Adequate board oversight is vital in today's environment, but what does "adequate" mean. According to one publication: "Directors may delegate many of their powers to others, such as officers and employees, but the directors are ultimately responsible for all corporate decisions."[4] In other words, the buck stops with the board. One of the ways that board members are responding is by seeking greater assurance from management that the institution is being operated ethically and effectively. A comprehensive risk management process that includes board-level input and oversight is a tool that can help provide this assurance.

However, a diligent board often feels caught in an endless loop. The more the members know, the more they understand the enormity of what there is to know. A comprehensive and coherent process for identifying, assessing and planning responses to risks that is based on explicit institutional objectives should be part of what a knowledgeable board expects management to have in place. This is a must in order for the board to become comfortable that their oversight activities adequately protect stakeholders' interests.

What happens if board members and officers do not manage risk effectively? The failure to manage risk has resulted in large financial penalties and reputational damage to many prominent colleges and universities. For example, scanning recent headlines of *The Chronicle of Higher Education*, we find multimillion dollar fines, legal settlements or damaging publicity related to:

- Misuse of federal grants
- Inappropriate billing for medical services
- Research abuse and fraud
- Underpayment of royalties
- Apparently lavish spending by executives
- Athletic tutoring and recruiting abuses
- Unsafe laboratory conditions and handling of hazardous waste
- Scientific misconduct and student plagiarism

Risk management does not guarantee that such events will not occur, but it does reduce the chances of embarrassing headlines and significant financial penalties. A comprehensive approach to risk management provides reasonable assurance that an institution understands and manages the risks it faces—thereby better protecting reputation and the interests of its stakeholders.

Charitable reform legislation

National charity reform legislation continues to be a possibility, although at one time it appeared to be imminent. In 2004, 2005 and 2006, the Senate Finance Committee and the House Ways and Means Committee held several hearings about the need for greater oversight of charities. Independent Sector, a coalition of nonprofit organizations, established the Panel on the Nonprofit Sector to propose self-regulation. But comprehensive federal-level legislation has not been enacted, although several reforms and charitable giving incentives were included in the pension reform bill that President Bush signed into law in August 2006. For example:

- Effective for returns filed on or after August 18, 2006, §501(c)(3) institutions must make their Forms 990-T available for public inspection.
- Payments of interest, royalties, annuities, or rental income from a controlled organization will no longer be taxable to the controlling organization provided that the payments were: 1) made pursuant to a binding written contract that was in effect as of August 17, 2006, and 2) received or accrued after December 31, 2005 and before January 1, 2008. Nevertheless, payments shall be taxable to the extent that they exceed fair market value.
- Controlling organizations must report on their Forms 990 income from and loans to, controlled organizations as well as transfers between controlled and controlling organizations. This provision is effective for returns due (without regard to extensions) after August 17, 2006.

Several states also proposed legislation that was designed to increase the accountability of nonprofits, and a few enacted it. For example, California was an early adopter, passing its Nonprofit Integrity Act in 2004, which became effective on January 1, 2005. It requires charities with gross revenues of $2 million or more to undergo an independent audit of their annual financial statements and establish an audit committee comprised of independent members. However, a charity that is operated primarily as an educational institution, hospital, health care service plan, or a religious organization is exempt from the independent audit and audit committee provisions of the Act.

Other states, notably New York and Massachusetts, proposed legislation that still has not been enacted. In New York, the Attorney General proposed several pieces of legislation in 2005. Two key bills (# AO7824 and AO7825) were passed by the Assembly and delivered to the Senate but then referred to committee in June 2006. In Massachusetts, the Attorney General proposed financial integrity legislation in 2005 but in June 2006, it was sent to the committee on Consumer Protection and Professional Licensure for further study.

New standards raise the bar

The AICPA, the national professional organization for certified public accountants, issued its Statement on Auditing Standards (SAS) No. 112, *Communicating Internal Control Related Matters Identified in an Audit*, in May 2006. SAS 112 adopts new definitions for internal control deficiencies and presents specific examples of situations that auditors should classify as “significant deficiencies”[5] or “material weaknesses.”[6]

As a result of SAS 112, auditors will need to categorize more existing circumstances as significant deficiencies or material weaknesses and communicate them to external and internal stakeholders. Of most relevance to this paper, if an institution has an ineffective risk management program, the auditor will need to conclude that the institution has a material weakness in internal control, which is the most severe type of deficiency.

In addition to SAS 112, the AICPA issued eight new SASs (i.e., SASs 104 to 111) in 2006 relating to the assessment of risk in a financial statement audit. The new SASs provide for more:

- In-depth understanding of the auditee's environment, including its internal controls, to help the auditor identify risks of material misstatement in the financial statements.
- Rigorous assessment of those risks and the effectiveness of the steps the auditee has taken to mitigate them.

Along with SAS 112, the new SASs are cause for attention in the education and nonprofit sector because auditors are required to follow them for audits of all types of organizations. Other guidance (e.g., the Public Company Accounting Oversight Board or PCAOB) is only applicable to auditors of companies that issue publicly traded securities. Essentially, the new AICPA SASs all but eliminate differential treatment of not-for-profit organizations by auditors as compared to organizations that are publicly traded.

How is ERM implemented?

Are institutions embracing enterprise risk management? In our experience, board members and officers are focusing on broader institutional risks, including financial, reputational, operational, and strategic risks. A number of universities have designated an individual to be responsible for risk management. Fewer have performed an entitywide risk assessment, and fewer still have a defined plan to make enterprisewide risk assessment and response a formal, sustainable process.

One possible reason that the ERM model has not gained more traction within the higher education and not-for-profit sectors is that it may seem difficult to translate the theory into a step-by-step action plan. Another reason may be that effectively implementing ERM requires the naming of a leader to move the program forward. This leader will need to devote substantial up-front time to designing a model tailored for the institution and identifying key players who can make the plan work. Without very strong endorsement from senior leadership it may be difficult to take such a person "offline" from existing duties.

Here are two ways to go about developing a framework for ERM. The first (at right) relies on the COSO model, and the second (on page 16) uses an existing parallel model.

1) Using the COSO model

The implementation process will need to be driven from the top-down in the institution and must have the support of the board and the president. Risk management is not solely a "finance" issue and if it is portrayed as such, implementation is less likely to succeed. Figure 2 provides a list of who should be involved in the implementation process and it suggests their responsibilities.

Figure 2:
Who should be involved? What responsibilities should they have?

Who to involve	*Responsibilities*
Board members	■ Supporting the design and operation of ERM in the institution ■ Understanding key objectives and related risks ■ Monitoring the process ■ Provide oversight for risk management activities
President and Provost	■ Endorsing ERM objectives and the implementation plan ■ Supporting ERM leadership in their roles ■ Communicating the value of ERM processes to the academic community
Officers	■ Designing the framework ■ Assessing the institution's ERM capabilities ■ Considering how the officers conduct business in light of the framework component ■ Identifying risks in areas under their responsibility
Internal auditors	■ Working with management to design the framework ■ Offering ideas and suggestions, since risk language is their area of expertise ■ Educating the institution about risk and facilitate discussions ■ Providing periodic monitoring of the process and its outcomes
Functional leaders	■ Ensuring key functional areas such as treasury, HR, finance, development, student affairs, athletics, payroll and taxation and so on are involved in the process providing their thoughts on risk as encountered in their daily activities and aiding with implementation

The key stages of the implementation process mirror the eight components of ERM (i.e., internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, monitoring). The key stages are as follows:

Understand the institution's internal environment.

The internal environment encompasses an institution's ethical values, philosophy for managing risk, human resource policies, and overall organizational structure. These elements establish a tone within the institution that represents management's beliefs and attitudes, which are captured in internal policy statements, such as the institution's code of conduct.

The internal environment starts at the top of the institution and flows down. Management must have a commitment to competence that is reflected in its policies and daily operations. An ineffective control environment can lead not only to operational inefficiencies, but also to reputational risks.

The governing board is crucial to establishing the proper tone at the top. There is a strong link between good governance and effective risk management. Board members bring unique characteristics to the institution, act as independent overseers, and serve as checks and balances on management. Boards should take an active role in the ERM process and ensure that management is implementing it effectively. Officers should update board members regularly and discuss the benefits they are realizing as well as the challenges they are encountering.

Establish overall ERM objectives as well as objectives by type (i.e., strategic, operational, reporting and compliance).

What are we hoping to accomplish with ERM that we would not be able to accomplish otherwise? Ask this question and answer it thoughtfully because without a clear sense of purpose, an ERM program will not be successful. For example, overall objectives might be:

- Defense: As a means of anticipating problems before they occur and threaten the institution's strategic objectives
- Coordination/integration: As a way to break down internal barriers of communication and promote greater coordination and efficiency throughout the institution surrounding the risk management process
- Exploiting opportunities and creating value: As a way to understand how risks interact across the institution and develop ways to prevent, react to, and create value for the institution by recognizing new opportunities

The objectives should be concrete, measurable, and widely communicated. They should be linked to performance measures and the institution's strategic objectives. Examples of objectives by type might include the following:

- Strategic objectives are high-level goals that are aligned with and supporting the institution's mission. For example, an institution's strategic objectives may be to:
  - Secure the resources needed to achieve its mission through a variety of sources and use them prudently.
  - Promote interdisciplinary and collaborative learning, teaching, and research.
  - Create an environment that promotes a culturally diverse campus community.
- Operational objectives are directed at using resources effectively and efficiently. For example, an institution's operational objectives may be to:
  - Achieve a target enrollment of X students for the 2007/2008 academic year.
  - Decrease its tuition discount rate by X% by the 2007/2008 academic year.
  - Implement a complete Enterprise-wide Resource Planning (ERP) information system solution by the fall of 2007.
- Reporting objectives are concerned with the reliability of internal and external reporting. For example, an institution's reporting objectives may be to:
  - Provide weekly budget updates to departments for their review.
  - Ensure that effort reporting is complete and accurate.

- Provide the board with meaningful data to assess the institution's financial performance on a timely basis.

- Compliance objectives are directed at specific actions that must be taken to comply with relevant laws and regulations. For example, an institution's compliance objectives may be to:
  - File grant reports with federal sponsors in a timely manner.
  - Maintain a complete list of federal laws and monitor the campus' compliance with them.
  - Develop a detailed policy for preaward and postaward activities.

While objectives in these four areas are important, many higher education institutions, especially research universities, may realize the greatest return on investment by focusing first on compliance risk. Risks that might mar an institution's reputation and brand also are vitally important. For example, intercollegiate athletics programs might not be significant from a financial perspective but they often represent very significant reputational risks.

Identify risk events that could impair the institution's ability to achieve its objectives

This step involves bringing together key personnel from many levels within the institution to brainstorm and developing a list of the various institutionwide risks. Use the risks in Figure 3 as a starting point.

Figure 3:
External and internal risks[7]

External risks
(e.g., related to donors, sponsors)

Economic
Availability of capital
Debt rating
Investment return
Unemployment
Interest rates
Competition

Environmental
Pollution control
Ability to handle natural disasters
Energy costs
Disposal of waste

Political
Government regulations:
federal, state, and local
Legislative policies
Public policy
Neighborhood relations

Social
Demographics
Student and parent behavior
Terrorism
Privacy

Technological
Emerging technology
Data security
Interruptions

Internal risks
(e.g., involving students, faculty and staff)

Infrastructure
Availability of assets
Access to capital
Institutional structure:
multi-campus, international, etc.

Personnel
Employee capabilities
Health and safety
Organizational structure
decentralized responsibility

Process
Formal policies and procedures
Integration of key business functions
Rigor of central administration, and
fiscal management
Software and ERP implementation impact

Technology
Data integrity
System usability
Usefulness of data
System maintenance

Compliance matters
Charging costs to sponsored projects
NCAA rules and regulations
Taxability of benefits
Human subjects
Scientific conduct
Detecting plagiarism
Charging to gift funds

Another approach is to consider objectives in each of the following broad activity areas on your campus:

- Educating students
- Managing enrollment and financial aid
- Managing endowments and investments
- Maintaining quality and compliant athletic programs
- Developing funding sources
- Delivering quality services to students (and staff)
- Managing construction, facilities and public safety
- Conducting and administering research
- Utilizing information technology effectively and strategically
- Hiring, deploying, and developing human resources
- Providing patient care and billing payors
- Managing financial operations
- Managing legal and compliance matters
- Managing external relationships
- Managing international programs and initiatives
- Planning strategically for the future

For each of these areas it is possible to identify key strategic, operating, reporting and compliance objectives—and the related risks that impede their achievement. Employees at all levels could help develop the list of risks. Also, both external auditors and internal auditors should be asked for their input. The list should include institutionwide risks as well as those at the individual school or campus level and at the departmental and functional level.

One technique for identifying risks is to conduct interviews with employees throughout the institution to get their perspective on risk. Questions often focus on the "messages" inherent in the control environment; key unit and department objectives and threats to achieving them; areas where the interviewee believes there may be problems; and the availability of accurate and timely information to facilitate managing risks. Surveys are another technique. The risks identified can then be presented to a central "risk steering committee" that prioritizes the list.

One major pitfall to guard against is "risk overload." Assembling a wide cross-section of knowledgeable employees to brainstorm about risks can produce outcomes that are so overwhelming that they can potentially create "risk paralysis." For example, one institution developed a 60-page catalog of laws and regulations to which it was subject. Sound change management principles apply here and the ERM project leaders must find ways to create manageable lists of consensus-driven key risks that can be prioritized and translated into actionable plans.

In addition, management should determine its "risk appetite" at the entitywide level. As noted earlier, an institution's risk appetite is its assessment of how much risk it is willing to accept in order to realize the anticipated benefits. Many corporations measure their risk appetite relative to profit. In higher education, it might be more appropriate to consider risk relative to such benefits as increasing research activity from "high" to "very high."

Other examples include:

- In order to reduce its student/faculty ratio, would a university accept the risks of having more adjunct faculty and/or limiting student enrollment?
- In order to improve its selectivity, would a college accept the financial risk of enrolling fewer students?
- In order to increase retention rates, would an institution accept the risk of extending more assistance to financially challenged freshmen?

Conduct a risk assessment of identified entitywide risks.

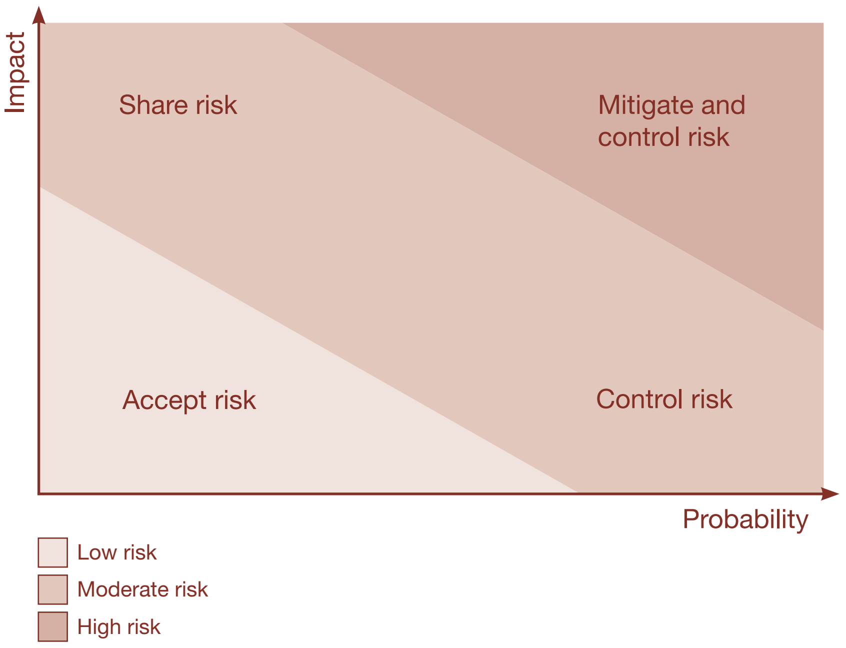
A comprehensive risk assessment would be best practice. However, for many institutions a comprehensive assessment might be too costly and it might result in risk overload. It might be more practical to start with known risks. Many business officers, especially those with a history at the institution, would be able to readily identify significant risks that would make good starting points. Departmental administrators and functional business unit leaders are critical resources in identifying risks in their units, assessing them and elevating them to their supervisors.

Once risks have been identified, an institution needs to determine the probability of them occurring as well as the impact they might have. Figure 4 shows a risk map.

Figure 4 plots risk in terms of its probability and impact. For example, if a risk has a low probability of occurring and a moderate to high impact, the institution would likely be willing to accept or share the risk. However, many university reputational risks might be in this category, and they would be more difficult to share (e.g., students studying abroad who might be impacted by a terrorist attack).

The choice is more difficult when a risk has a high impact and a high probability of occurring. Under ERM, an institution can find ways to mitigate risk by, for example, strengthening internal controls.

Figure 4:
A risk map



Develop a response to the risks.

Now that the risks have been identified and assessed, revisit the objectives set during Step 2 and develop a response. As described in the following four bullets, the choices include accepting, controlling, sharing or mitigating the risks. (See the four choices plotted in Figure 4 above.)

- Accept: When the impact and probabilities are low, the institution might accept the risk as is, concluding that it does not need to control, share or mitigate it.
- Control: The institution recognizes that a high probability for a given risk occurring exists, but the impact is low and proper controls are in place to handle the risk.
- Share: When the impact is high and the probability is low, the institution might decide to shift some of the risk to others (e.g., insurance companies, cooperative agreements).
- Mitigate: When the probability and impact are high, the institution might decide to design processes to reduce and control its exposure to the risk.

Based on the outcome of the above analysis, management should consider the costs and benefits of its possible responses, develop a budget, and assign accountability for carrying out the responses. Also, it is a good idea to start by developing a response to a finite number of risks. After achieving some successes, the ERM program can be expanded to include responses to other risks.

Establish control activities, such as policies and procedures, to make sure that management's risk responses are carried out as intended.

While some institutions rely on an existing group (e.g., internal audit, or a compliance committee) to be a catalyst to build early momentum for an ERM process, we believe the best long-term model is to establish a new, ERM-specific risk management committee. This group often includes members of senior management, and several of the individuals who were part of the risk assessment process, as well as other employees and administrators.

The risk management committee should be responsible for coordinating individual risk management activities within the institution. It might act as a technical resource and advisory body, gathering information and assessing and providing recommendations to senior management and the president, or serving as a strategic body responsible for developing and managing a comprehensive, integrated risk management plan.

In addition to the risk management committee, some institutions might consider a position for a risk officer who would report to senior operating management and who would advise and provide risk management training to departments.

It is important to remember that everyone is responsible for risk management, not just the members of the risk management committee. While ERM needs a leader, the key to success is involving as many people as possible in the process. If employees spot a risk or an opportunity they need to know where to turn and be encouraged to voice their thoughts, ideas, and opinions. Also, make sure that risk responsibilities are incorporated into employees' formal goals for the upcoming year and hold them accountable for achieving them. If risk responsibilities become long-term expectations, then make sure they are built into employees' job descriptions.

Initial risks should continue to be assessed and monitored institutionwide. Also, since institutional, departmental, school and functional unit objectives are dynamic and ever-changing, there will be new risks to be identified, assessed and managed.

Finally, effective risk management and effective internal controls go hand-in-hand. A best practice would be to enhance the internal controls around the areas of highest risk.

Capture relevant information and communicate it widely.

Individuals within the institution need information in order to manage risks. Information needs to be identified, captured, and communicated in a form and on a timely basis that enables them to carry out their responsibilities. Communication may be informal (e.g., one-to-one conversations) or formal (e.g., policy manuals) or technology-enabled (e.g., intranet site).

Management communications should focus on behavioral expectations and the responsibilities of personnel. They should include a clear statement of the institution's risk management philosophy and approach as well as a clear delegation of authority. Embedding the risk management philosophy into the institution's culture requires top-down communication of philosophy and expectations that is supported by bottoms-up information flows.

Information provided should be responsive to the following critical questions: What are the key performance indicators related to our major objectives? What key risk indicators provide a top-down perspective of potential risks? What data are required for the performance metrics? What level of information granularity is appropriate? How frequently does the information need to be collected? And distributed? Where and how should data be obtained?

Monitor the progress of the ERM program.

Revisit the objectives established at the beginning of the process, and determine if progress is being made. Monitoring should be an ongoing process. Over time, some risks may be adequately addressed, and new risks may take their place. The scope and frequency of the monitoring depends upon the risks and the related controls that are in place. For example, high risk areas may need to be monitored more frequently.

Also, institutions should develop a method to deal with deficiencies that are noted throughout ERM implementation and monitoring. A deficiency can be defined as any failure to adequately identify or mitigate an issue that affects management's ability to meet its objectives. Deficiencies should be discussed with superiors and significant issues should be reported to the board.

Monitoring should also involve evaluating the choices and outcomes of risk responses. For example, are our risk-sharing activities cost-effective? Do we develop mitigating controls that work to control risk without creating undo burdens on operating personnel?

2) Building from an existing parallel model

Many academic medical centers and large, multi-campus public universities already have a process in place that very closely parallels the ERM model—that is, comprehensive institutionwide compliance programs. It is easy to see the parallels between compliance programs and ERM processes, in that ERM extends the compliance program model to also embrace the other categories of risks faced by an institution (i.e., strategic, operating, and reporting risks.) The Office of Inspector General (OIG) of the Department of Health and Human Services (HHS) issued guidance for recipients of awards from the National Institutes of Health (NIH) and other agencies of the U.S. Public Health Service (PHS) regarding components of an effective compliance program.[8] We will use the elements of a compliance program outlined there to step through how an ERM could be implemented by extending the compliance program model to cover all risks.

The eight basic compliance program elements outlined in the OIG guidance are:

1. Developing and distributing written standards of conduct and written policies and procedures that reflect the institutional commitment to compliance

2. Designating a compliance officer and forming a compliance committee

3. Conducting effective training

4. Developing effective lines of communication including anonymous capabilities available to all personnel

5. Auditing and monitoring the design and outcomes of the program

6. Enforcing standards through well-publicized disciplinary guidelines

7. Responding to detected problems and developing corrective action initiatives

8. Establishing roles and responsibilities and assigning oversight responsibility

The compliance model included in the OIG guidance—as well as successful compliance programs already in place at numerous academic medical centers and large universities—are built upon the concepts we set forth at the outset of this paper. That is:

- The array of objectives and therefore risks is very broad.
- Information and management must come from all ranks of the institution, not simply the executive suite.
- People within the institution understand a vast majority of the barriers to achievement of its objectives.
- Relevant risk information must flow up, down and across the institution; also, anonymous channels can be important to the process.
- While not all risks can be avoided, most surprises can be minimized.
- Institutional activities and objectives are ever-changing, and thus the program must be dynamic and continuous.

While extending many of the eight elements listed above from a compliance program to an ERM program becomes relatively intuitive by changing the word "compliance" to ERM, some areas for further explanation and comment are:

- The compliance officer may become the chief risk officer, and the compliance committee may become the risk management committee. Alternatively, there may be two "chief officers" and two "committees." The following questions suggest some of the choices that will need to be made.
  - Does the compliance officer become the chief risk officer, or does he/she report to the chief risk officer?
  - How much of the membership of the internal management compliance committee also serves on the risk management committee?
  - Does the chief risk officer report to the same university executive as the compliance officer?
  - Where does the responsibility for risk management oversight reside at the board level, and does this make sense in light of board oversight of the existing compliance program?
- The compliance committee will need members whose experiences and insights encompass strategic, operational, and reporting responsibilities as well as compliance issues.
- Don't underestimate the importance of training. New employees need training, but so do long-term employees to reinforce expected behaviors and to learn new behaviors.
- The anonymous reporting of compliance issues may well need to be extended to include other matters. However, this presents logistical issues and runs the risk of confusing the community. One answer may be to establish a new broad-based anonymous reporting mechanism for risk matters and to reposition/redefine the compliance mechanism that already exists.
- Enforcing standards seems applicable most clearly to compliance matters. However, once roles and responsibilities are defined and training is in place, committing fraud or wasting resources can also be seen as requiring disciplinary action. Similarly, the failure of a responsible employee to detect such activities within their functional unit may be grounds for action.

In the final analysis, we believe that an institution that builds its ERM process by extending the base of a preexisting effective compliance program model will ultimately arrive at the same destination—an ERM process that is grounded in the COSO framework. This can be seen by a mapping of the eight elements of a successful compliance program in the OIG guidance document to the eight components of the COSO framework in Figure 5 on the next page.

Figure 5:
Key ERM features

Compliance program element per OIG:	*COSO ERM framework components:*
1. Written standards of conduct; policies and procedures	Internal environment; communication
2. Compliance officer and compliance committee	Internal environment; control activities
3. Effective training	Control activities; communication
4. Effective lines of communication	Information and communication
5. Auditing and monitoring the design and outcomes	Monitoring; control activities
6. Well publicized disciplinary guidelines and enforcement	Control activities; communication; internal environment
7. Responding to detected problems and developing corrective actions	Risk identification; risk response; control activities
8. Assigning oversight responsibility; establishing roles/responsibilities	Internal environment; control activities; communication

What is the role of internal audit?

Internal auditors have a professional responsibility to assist their institutions in risk management efforts.[9] They recognize that risk management is an important business process, and it should be evaluated in a manner similar to other strategically important processes. Further, an effective internal audit function performs risk assessment processes in the course of determining its audit plans. The results of these risk assessments can and should inform and be informed by the ERM process.

Internal auditors are also trained to understand the role of internal controls in assuring the attainment of strategic, operational, reporting and compliance objectives. As a result, based on their skills as well as their broad knowledge of the institution, the internal auditor and his/her staff are significant resources that should not be excluded from the design and implementation of ERM.

Internal audit, in its role as a primary monitor of control effectiveness, will eventually need to evaluate the adequacy of the ERM process. Like external auditors, internal auditors are precluded from auditing their own work by professional standards. However, internal auditors can assist in identifying, evaluating and implementing risk management methodologies and controls to address identified risks.

These broad role descriptions may translate into internal audit championing the establishment of an ERM process; facilitating identification of risks; advising on appropriateness of responses; consolidating the reporting of risks; and participating in presenting the overall risk strategy for board approval. Care should be taken, however, to respect the chief auditor's judgment as to permissible roles and where the lines must be drawn. It is also vital to assure that the chosen advisory services are allowed under the institution's internal audit charter and understood by and agreed to by the board's audit committee.

Management and the board are responsible for the institution's risk management and control processes. While internal auditors can—and arguably should—facilitate risk processes, they cannot be responsible for the management of the risks identified through that process. Their highest role is to assist management by evaluating the effectiveness of its risk management efforts, a role which requires appropriate independence and objectivity.

ERM is a best practice
and the “right thing” to do.

Effective ERM is an ongoing process that requires strong commitment from upper management and collaboration between cross-functional units. An effective risk management process must become embedded in the culture of the university, and it must include staff, faculty, administration, and students. Education and awareness efforts should be aimed at each of these constituencies. ERM is not just another "project" to undertake, but rather represents a continuous commitment to improvement through a formal, self-renewing process.

ERM also is a best practice. The COSO framework reminds us that all entities exist to enhance value to their stakeholders. The continuous identification, assessment, mitigation and monitoring of risk is critical to protecting, maintaining, promoting, and enhancing stakeholder value. ERM directly supports this initiative and allows an institution to minimize their risks and align their risk response strategies with the key objectives of the institution.

No matter how thorough an ERM process is or how prominent it is throughout the institution, risk can never be eliminated, as it is inherent in most activities. ERM, however, is a strategic management technique that can enable an institution to operate more efficiently and effectively in both its current and prospective environment.

Despite all of this analysis, ERM is not new (in fact, this paper updates an earlier discussion from 2001[10]). As a result, some may well ask, "Why now? What is the new value proposition?"

We believe that expanded post-Sarbanes accountabilities, the ever-growing complexities of educational institution initiatives, both nationally and globally, the possibility of charitable organization reform legislation and the new AICPA Standards for evaluating control effectiveness are current elements that argue in favor of a structured ERM process.

However, we contend that the need to protect the varied interests of an institution's many stakeholders and the inherent complexity of an organization's operating activities are the overarching factors that make ERM a best practice … not just a possible approach. It is the "right thing" to do.

How then to move the ERM question from an intellectual debate or a theoretical argument to a value-adding reality?

Today, we often see that the board has become a major driving force for ERM implementation. Here, then, from an oversight perspective, are the elements that an ERM model "must have" to make it worth the considerable investment in time, people and financial resources that it will require:

- Make ERM a priority. To succeed, this cannot be yet another initiative from a corner of the campus that competes for time, attention and resources. The board and the executive suite must be fully on board with the process and sold on its value. And they must communicate this support early and often.

- Make ERM align with key institutional objectives. A well-run institution knows its goals and communicates them widely and effectively. Aligning ERM with critical objectives to help assure that they are achieved provides evidence of value and sets ERM apart from most other campus "projects."

- Make ERM manageable. One sure way to doom the project is to create "risk overload." The early objective is not to build an exhaustively impressive list of possible risks. Instead it is to talk publicly and constructively about critical risks that are well known around campus, and develop a process for defining meaningful responses. Start with a finite number of risks to prove that the process works and is worthy of being extended.

- Make ERM measurable. To be meaningful, objectives at the institutional, school, department or unit level should be defined in a way that makes them measurable. Objectives carry with them risks that must be identified and assessed, which then become the basis for actionable responses. Responses must align with defined risk tolerances. By following these principles, the ERM process and its outcomes will be measurable.

- Make ERM actionable. The COSO framework builds to a list of responses to specific, prioritized risks. Properly implemented, the question at the end of an ERM cycle is not "What do we do"? But, more properly, "Which ones do we take on now, and which ones come next?"

Implementing an ERM model that meets these objectives will reduce the risk of reading embarrassing headlines about your institution and maximize the protection of stakeholders' interests. By adding value in these key ways, your ERM process will also assuredly become self-sustaining.

Endnotes

[1] Risk appetite is defined as management's view of how much risk an institution is prepared to accept in order to achieve its objectives.

[2] From the Executive Summary of *Enterprise Risk Management—Integrated Framework*, page 2, at www.coso.org.

[3] To make this depiction more directly applicable to higher education, we have changed the original descriptors in the COSO document on the right face from "Entity-Level," "Division," "Business Unit," and "Subsidiary" to "Institution," "School," "Department" and "Functional Unit."

[4] From the California Attorney General's *Guide for Charities*, published by the State of California in 2005. It is available at: http://ag.ca.gov/charities/publications.htm.

[5] A significant deficiency "is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected." (SAS 112, paragraph 6)

[6] A material weakness "is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected." (SAS 112, paragraph 6)

[7] Adapted from COSO's *Enterprise Risk Management—Integrated Framework*, which can be found at www.coso.org.

[8] "Draft OIG Compliance Program Guidance for Recipients of PHS Research Awards," dated November 28, 2005. See *Federal Register* Volume 70, No.227 of November 28, 2005, beginning at page 71312.

[9] This discussion is informed by a reading of three Institute of Internal Auditors *Practice Advisories: Advisories 2100-4 and 2110-1* (both dated March 2001) and *Advisory 1000.C1-1* (dated May 2001).

[10] In 2001, PricewaterhouseCoopers and NACUBO published *Developing a Strategy To Manage Enterprisewide Risk in Higher Education*. This paper presented risk management theory, examples of approaches being taken by the for-profit corporate sector, and results of discussions held with higher education leaders about managing risk effectively in the higher education environment. Interested readers can find this paper on our web site at: www.pwc.com/education. Look in the "publications" section.

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 other types of not-for-profit organizations.

Dale L. Cassidy is a director in PricewaterhouseCoopers' Education Advisory Services practice with over 19 years experience with the firm. He specializes in advising colleges and universities about risk and control issues.

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 to build public trust and enhance value for its clients and their stakeholders. More than 130,000 people in 148 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

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

www.pwc.com/education