Meeting the Challenges of Enterprise Risk Management in Higher Education

AGB ASSOCIATION OF GOVERNING BOARDS OF UNIVERSITIES AND COLLEGES

NACUBO

In the summer of 2007, the Association of Governing Boards of Universities and Colleges (AGB) and the National Association of College and University Business Officers (NACUBO) held a summit on enterprise risk management (ERM) in Washington DC with senior officers and trustees from several leading colleges and universities. Approximately 40 leaders—representing large and small as well as public and private institutions—attended the event. (For a list of attendees, see page xx).

The summit opened with a presentation on implementing ERM in the for-profit financial services industry. The next morning the group heard four perspectives on risk management from a trustee, a chief risk officer (CRO), a president (CEO), and a chief business officer (CFO). After that, the group worked as a whole to develop a higher-education-specific model.

The objectives of the summit were to begin to develop a robust, sustainable ERM model for colleges and universities, and to identify the appropriate ERM roles for presidents, CFOs and other senior managers, and trustees from large and small, public and private institutions.

PricewaterhouseCoopers LLP, IBM, and United Educators Insurance, a Reciprocal Risk Retention Group generously supported the summit. NACUBO and AGB are grateful for this support, which allowed the associations to make progress in development of an ERM model for higher education.

Special thanks to John Mattie of PricewaterhouseCoopers, whose vision inspired the summit and who served as primary author of this paper.

Introduction

Risk can be defined as any issue that impacts an institution's ability to meet its objectives. The Committee of Sponsoring Organizations, known as COSO,[1] defines enterprise risk management (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**, to provide reasonable assurance regarding the achievement of entity **objectives**." [2]

Several words in COSO's definition are highlighted for emphasis: process, strategy, risk appetite, and objectives. ERM is a continuing process that aligns with strategy and changes as the institution's activities and objectives evolve. Risk appetite is defined as management's view of how much risk an institution is prepared to accept in order to achieve its objectives. Like investors, some institutions are more comfortable with risk than others.

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

1. Strategic – high-level goals that are aligned with and support the institution's mission
2. Operational – ongoing management process
3. Financial – protection of institution's assets
4. Compliance – the institution's adherence to applicable laws and regulations

Reputational risk is often included as a critical higher education risk. Summit participants agreed that a serious event in the above listed categories can cause reputational risks.

ERM has 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."

1. Internal environment – the culture, values, and environment in which an institution operates
2. Objective setting – the process that management uses to set its strategic goals and objectives

1 COSO is "a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance," according to the organization's Web site. In the late 1980s, COSO conducted a study to define and advance the understanding of internal controls that resulted in the report, *Internal Controls—Integrated Framework.* In 2004, COSO released its report, *Enterprise Risk Management—Integrated Framework.*

2 *Enterprise Risk Management—Integrated Framework,* published by COSO in 2004.

3. Event identification – internal and external events that could affect an institution's ability to achieve its objectives
4. Risk assessment – assessment of the impact of risks and prioritization of those risks
5. Risk response – how management will respond to the risks an institution faces (e.g., mitigate the risk, or share the risk)
6. Control activities – policies and procedures that an institution establishes to ensure that it responds to risks
7. Information and communication – identification and communication of the right information to the right people
8. Monitoring – monitoring and taking corrective action as needed

To be successful, risk must be managed across the four objectives, the eight components, and at each organizational level (i.e., functional unit, department, school, and the institution as a whole). Risks cannot be eliminated, but ERM can enable an institution to manage them more efficiently and effectively.

These definitions and concepts are critical to an understanding of ERM. We will refer to them throughout the paper as we present the results of the AGB/NACUBO ERM Summit.

Components of a higher-education-specific ERM framework

In this section, we examine the eight components of the ERM framework from a higher education perspective, as fleshed out by the ERM Summit participants.

Internal Environment

The internal environment is the basis for how risk is viewed and encompasses the institution's culture, tone, and values. The environment is revealed through internal documents, external communication, the actions of insiders, and other indicators. The environment, for example, is reflected through the organization's code of conduct, management's leadership, communication and decision making style, or in the governing board's actions.

Summit participants stressed that simply having mechanisms such as a code of conduct or conflict of interest policy is not sufficient. The key is whether or not the institution's culture will tolerate noncompliance at any point within the institution with its written or implicit codes, ethics, and policies. As one participant said, "checking the box is not enough."

Training that addresses risk concepts can help create the desired culture. Summit attendees thought that emphasizing training would be a visible and action-oriented way to impact the organization. Further institutions should develop training on expected behavior for new and existing employees. Both groups need to know what is expected and what will not be tolerated. Training should begin at the level of academic deans, department heads, business managers, and administrators. Finally, a robust and thorough communication plan should complement and reinforce the training curriculum.

Objective Setting

Objective setting means that management sets goals that align with the institution's mission and its appetite for risk. Participants generally agreed that the best place for ERM to begin is with strategy. Strategy is the glue that binds the approach to the objective – and an institution's approach should take risk into consideration. For example: Why does the institution want to build a new science lab? What will happen if the institution does not build a science lab? The proposal to build the science lab should consider the return on investment (ROI) risk in qualitative and quantitative terms.

Consider, too, the objectives of initiatives that are already in process, such as an architectural school that was built 10 years ago but continues to struggle with enrollment. A good time to review such initiatives is during the planning and budgeting process. Should the institution continue to fund the initiative? If the initiative is of demonstrated strategic importance, will increasing the funding for two to three years enable it to succeed?

The organizational structure of colleges and universities has to be taken in consideration. Buy in is critical at all levels, from the board to the president to faculty and administrators.

Employees at all administrative levels of the institution also need to understand how they fit into the strategy. When implementing a strategic initiative, the payroll department, for example, needs to understand its role. How does payroll fit into the institution's plan to implement a new information technology system?

Participants at the ERM Summit questioned: "What are the most urgent risk objectives?" For example, is compliance such a hot topic that it needs to be at the top of the list for every research university? The participants agreed that institutions need to address all four risks: strategic, compliance, financial, and operational. What about reputational risk? Should it be the fifth type of risk? One person suggested that reputational risk is the risk of not managing the four objectives adequately.

Event Identification

Event identification requires the institution to identify activities that may impact its ability to achieve objectives. An important aspect of event identification is to distinguish risks from opportunities. Many institutions, especially those with academic medical programs or significant sponsored research, have implemented compliance programs. Such compliance programs have begun to lead some institutions toward an ERM framework. A growing number have conducted organizationwide assessments to identify risks.

Some institutions have found that a cross-discipline (and sometimes cross-level) risk committee that reports to senior management and/or the board can be very effective. The committee coordinates risk management activities and acts as a technical resource. Departments and units provide input to the committee on risks they have identified for assessment and response.

Summit participants stressed the importance of involving the campus community in identifying risks. One institution established an ERM committee of administrators who report directly to the institution's senior officers. This committee is working very well, partly because its members are closer to day-to-day operations and are in a good position to identify risks and to effectively manage them.

Another participant suggested that using words other than those in the ERM lexicon might be received better on college campuses. Rather than identifying "risks," consider identifying threats and opportunities. Many participants reported that campuses had made good progress in identifying potential risks, but most felt the process stalled at this point. A long list of threats or opportunities, numbering into the hundreds across an institution, can become daunting and lead to inaction.

Risk Assessment and Risk Response

Assessment involves analyzing the impact of identified risks; response addresses degrees of avoidance or acceptance of the risk. A "risk map," as presented in Chart 1, plots probability and impact of risk. It is a good tool for assessing the risks that have been identified and deciding how to respond to them.

In general, there are four responses to risk, which also are depicted on the risk map:

Accept – When the impact and the probability is low, accept the risk

Control – When there is a high probability of a risk but its impact would be low, ensure that appropriate controls are in place

Share – When there is high impact but low probability, share the risk with others (e.g., insurance companies, cooperative agreements, third party outsourcing)

Mitigate and Control – When both the probability and the impact are high, design controls and processes to reduce the exposure to the risk[3]

Chart 1: Risk Map

Summit participants agreed about two quadrants of the risk map. When both the impact and the probability is low (i.e., in the lower left quadrant), institutions would be likely to simply accept the risk. When both the probability and the impact are high (i.e., in the top right quadrant), institutions would be well advised to design controls that would, in totality, reduce the risk to an acceptable level. In this case, management would design appropriate controls under the oversight of the board.

The other two quadrants of the risk map present special challenges. In theory, when there is a high probability for a given risk but its impact is low (i.e., the "medium" risk in the lower right quadrant), an institution should ensure that controls are in place that would reduce the risk. Also, when there is a high impact but low probability (i.e., the "medium" risk in the upper left quadrant), an institution should consider sharing the risk with others. For example, institutions in the same geographic area could jointly share in a disaster recovery plan.

3 A fifth option is to reject the risk. An institution may decide not to do something because of the risk involved.

Summit participants agreed that the board and management should sufficiently discuss the two "medium" risk quadrants in particular. A key word is "sufficiently." If the risk event occurs, officers and boards should be able to explain the reasons for their decision. Summit participants examined several timely higher-education-specific examples of low probability/high impact events:

- a campus shooting like that at Virginia Tech
- another category 5 hurricane hitting New Orleans
- a pandemic flu outbreak

The board and administration should discuss and make contingency plans for such high-impact events of low-to-medium probability. In the case of the flu outbreak, should students be sent home and the campus closed? Is the campus health center prepared? Should they launch a campaign to inform students about how to reduce their chances of contracting the flu? Summit participants agreed that no planning would be worse than making conscious decisions to accept certain risks.

One participant suggested that institutions develop an "adaptable" response that could work for several high impact events. Another participant suggested that institutions should practice possible responses, especially to high probability/high impact situations. The practice, either through a table top drill or a full scale live event, would give institutions a chance to test and fine tune their planned responses.

Control Activities and Monitoring Activities

Control means that management requires adherence to policies and procedures that reduce risk. Examples of control activities are getting approvals or authorizations before making a purchase, reconciling bank statements, reviewing performance, or segregating duties. A standard practice is enhancing controls around the areas of highest risk. One example concerns written policies and procedures that describe how employees should carry out activities involving risky areas.

Monitoring, which is a follow up activity, ensures that the policies and procedures have been carried out as intended. If proper procedures have not been followed, management should take corrective actions. Both aspects—effective control activities and monitoring activities—are key to managing risks.

Sometimes monitoring procedures can be as simple as checking for a signature. Other times significant data and analysis is needed. Institutions may want to develop key performance indicators (KPI) for risks and controls. These financial and non-financial metrics would measure progress towards managing and monitoring risks. Institutions need to ensure they are working with the appropriate level of information granularity; not too much or too little.

Summit participants also stressed that controls are about accountability, and ERM is a framework that involves monitoring. Many acknowledged that there can be perfect controls yet risk isn't contained because management doesn't support monitoring. Attendees endorsed the importance of training. Such training must educate employees about organizational values, expectations concerning conduct, and the importance of control and monitoring activities. Training should also ensure that employees know how to implement the institution's policies and procedures to properly manage risk. Obviously, new employees need training, but it's also important for other employees to be reminded of existing policies and procedures or to learn about changes to them.

Information and Communication

Administrators and other members of the campus community need to have access to accurate information that is communicated widely. One participant brought copies of internal risk newsletters to the summit. Such newsletters (and Web sites) are good vehicles for communicating the successes of risk management as well as promoting new ways to continue to enhance it.

Written and verbal communications should educate and inform the community about why a new science lab, for example, is important to the institution's strategy. One participant said: "Sell the strategy, not ERM."

Risk newsletters also can serve as effective training tools. Participants emphasized the need for training for almost every aspect of the risk management process, and noted the need to "promote and educate" and "tell people why." Getting the buy-in of the campus community is very important.

A TWO-TRACK APPROACH TO ERM

The consensus at the ERM Summit was that there should be two separate "tracks" for ERM initiatives. The first, requiring an "offensive" position, would be for new initiatives. The second, more of a "defensive" position, would be for existing and ongoing programs.

New Initiatives

All of the components of the ERM framework should be addressed when management is presenting significant new initiatives to the governing board: 1) internal environment, 2) objective setting, 3) identifying risks, 4) assessing them, 5) responding to them, 6) developing control activities to mitigate the risks, 7) developing monitoring activities to make sure that the controls are applied, and 8) providing good information and communicating it widely and effectively.

The starting point for all new initiatives should be the institution's planning process. An ERM framework should be part of assessing and implementing strategies that relate to planned objectives. For example, if an institution is proposing to build a new campus in the Middle East, how does it align with the institution's strategy? How would the new initiative benefit the institution and what would be the consequences of not building it?

The majority of participants felt that a standard template to analyze all of the various risks associated with new strategic initiatives would be a useful tool for board members and senior management.

Continuing Operations

Most institutions do not have the luxury of managing risks from the ground up. Many initiatives are already in progress. How can ERM apply to existing initiatives? One participant noted that an "ERM filter" (i.e., a review of the eight components of the ERM framework) could be applied to ongoing programs to see how their chances for success could be improved.

One suggestion is to consider applying the ERM filter in the budget process. If the ongoing initiative is fundamental to the institution's strategy, has sufficient progress been made over the last year? If not, can funds be taken from a less strategic initiative and allocated to the higher priority initiative?

Janice Abraham, of United Educators noted, "There needs to be a lot of places to jump on the train and begin the process." Janice's observation is especially relevant to continuing operations. To apply ERM to continuing operational issues, institutions need to jump on the train where it is most appropriate and use ERM principles to deliver incremental value to existing initiatives.

In fact, many institutions are already using ERM but not calling it that. For example:

- Capital campaigns start with an analysis of risk. Benchmarks are identified. A quiet phase enables the institution to reduce its risk of not meeting campaign goals.
- Institutional compliance programs, which many research universities have successfully implemented, are an excellent model for ERM.
- Loss-prevention programs and insurance are components of a successful ERM program.

Such initiatives might be enhanced by using ERM. For example, an institution might be able to enhance its institutional compliance program if it reviewed the applicability of each of the eight ERM components. Summit participants agreed that the deans and directors, individuals responsible for building and managing departmental budgets and programs, are in the best position to identify, assess, and control risks of ongoing programs. Training is needed to help academic and administrative managers participate in the ERM process.

HARVESTING ERM

No matter what the initiative, institutions should identify relatively easy successes that they can build upon to help them prepare for the tougher challenges ahead. One participant used the term "harvesting" ERM. In other words, how can an institution reap early wins for risk management that can then help it achieve more wins down the road?

When looking for ERM opportunities, consider reviewing existing data for opportunities rather than compiling new data. Developing new data takes time and money, and the initiative might lose momentum during the process. Also, institutions already track much data. If they were to look at this data in a new way (i.e., using an an "ERM filter"), they can potentially identify ways to manage risk as well as to save costs and achieve greater efficiencies. Higher education's most significant costs relate to labor, and so reviewing existing data related to people costs (e.g., health and safety issues) is a good place to look for low-hanging fruit.

ROLES: WHOSE RESPONSIBILITY IS IT?

Everyone is responsible for risk management, and well-managed organizations involve people from different functional areas in risk management. To avoid duplication of effort and to make the process efficient, institutions should clearly define roles and responsibilities. We suggest roles for board members, presidents, chief financial officers (CFOs), chief risk officers (CROs), and others.

The Board

What is the role of the board in ERM? Frank Rhodes, Cornell University, described the board's role as: "noses in and fingers out." In other words, the board should ask appropriate, sometimes tough questions and in general, oversee. AGB advises, "Focus on policy rather than administration. A president needs a board that is engaged but not intrusive." [4]

In discussing potential new initiatives, boards should encourage management to consider ERM. Having the board focus on ERM reinforces its importance to the campus community. Also, a strong link exists between good governance and effective risk management.

One board member at the summit listed the following pre-conditions for a successful ERM initiative:

- The board must understand and have a commitment to ERM as a multi-year initiative.
- Management must truly be leaders. They must inspire those who work for them, and they must foster cultural changes to enable ERM to succeed.
- Every level of the institution from top to bottom needs to know how and why ERM applies to them. Leadership should address "WIIFM" (what's in it for me) upfront.
- Leadership also should: 1) support its case with cost/benefit analysis, 2) be prepared to invest in people and training, and 3) develop metrics to measure progress.

Another board member stressed the importance of setting priorities. For example, if an institution decides to provide more financial aid to students, then it must make cuts in other areas. An institution must live within its financial means, and one of the board's responsibilities is seeing that it does so.

The President

What is the role of the president? AGB says, "A president must engage both the faculty and the board in a partnership that yields effective governance and motivates the institution to meet the challenges of a rapidly changing world." [5] This dovetails nicely with ERM. The president should work with the board to set the high-level ERM agenda.

One president of a public institution who attended the summit described his ERM program, which is tackling some fundamental issues. This president believes that a crisis is building for public universities in his state. They cannot continue to increase tuition, and state funding is not likely to grow. As a result, the financial model must change. At the same time, public institutions have a responsibility to function as an economic catalyst in their regions and to become more entrepreneurial.

The president described one of his ERM initiatives, which turned these challenges into an opportunity. This institution receives approximately $14 million in taxpayer support for research, which was previously dispersed in amounts up to $90,000. The president established an external panel to disperse the money competitively based on the anticipated payback. In this case, the objective is to make the institution more entrepreneurial and an economic catalyst. The change starts from within.

4 *The Leadership Imperative* (page 33), published by AGB in 2006, is available on the association's Web site at www.agb.org.
5 *The Leadership Imperative* (page 38), published by AGB in 2006, is available on AGB's Web site at www.agb.org.

The Chief Financial Officer (CFO)

What is the role of the CFO? According to a study by the Associations of College and University Business Officers (including NACUBO), the chief business officer sets the appropriate tone, which stresses the importance of "ethical behavior, creating a trusting environment, and personal credibility built on effective interpersonal skills. At the heart of the chief business officer's job is the ability to communicate that he or she oversees a capable and principled operation." [6]

The principles of ethics and personal credibility are also at the heart of ERM. The CFO should be a key player who helps to establish and manage the ERM initiative, working with the president and the board.

One CFO who attended the summit described the ERM initiative in process at his institution. It began several years ago with the retirement of the business officer who was responsible primarily for insurance, facility risk, and safety. The CFO and his team decided to expand the role. Rather than risk management with a small "r" and a small "m," the new role would be implementing ERM.

The CFO hired a chief risk officer—someone from the corporate sector who had a vision of how ERM could succeed in higher education—to lead the institution's new initiative. With his help, the institution embarked on an extensive risk identification process. It established a committee whose members conducted extensive interviews as well as a detailed survey, and then developed a list of the top 10 risks. The process has been well received, and the CFO believes that this broad effort has built momentum for ERM that will help sustain it over the longer term.

The risk surveys and interviews identified universal risks such as individual safety (e.g., student or employee violence or terrorism), research risk, and an operational risk issue involving a unit that is very dependent on one sponsor.

The Chief Risk Officer (CRO)

What is the role of the CRO? The CRO is a leader, and sometimes a cheerleader of the ERM initiative. For example, one CRO at a large university system hosts an annual risk summit. Almost 350 people representing many campuses and medical centers attended the most recent event. Having them "own" risk management on their campuses helps to sustain its momentum. Working in groups, the participants exchange information and ideas they can bring back to their campuses to help drive ERM over the next year.

Each campus in this large public university system has an ERM committee. The committees analyze data to identify risk management opportunities, and thus far, the ERM committees are finding many opportunities to manage risk.

Technology is a significant component of this CRO's ERM vision, and it soon may play an even bigger role. The CRO is considering new technology that will provide dashboards so that departments or units can focus on applicable metrics. For example, each campus has a fleet of cars and trucks. The fleet administrator for each campus will track the ratio of the number of vehicular accidents to the size of the fleet. If the ratio seems high in comparison to that of other campuses, or if it increases over time, the system will implement solutions (e.g., a driver training program) that will provide an acceptable return on its investment.

6 "Cultivating Your Career," by Susan Jurow, *Business Officer,* June 2006 edition, is available at www.nacubo.org.

In some cases, the CRO reports to the CFO. In few instances, the CRO reports to the president or to the board (the audit committee, executive committee, or finance committee, although it would depend on the expertise of the committee members) or to both. Some find a dual reporting relationship encourages open dialogue.

One participant noted that it might not be appropriate for the CRO to report to the CEO at every institution. Some institutions are trying to limit the number of direct reports to the CEO. However, to be most effective, the CRO needs to involve all levels and functional units of the university, and the board must be supportive.

Several participants also felt that educational institutions might benefit from the identification of a university official who regularly looks for future "industry related risks" that may impact all of higher education. Examples of these endemic risks might be future declines in research funding related to certain disciplines, or brewing concerns by regulators over student lending practices.

The Chief Information Officer

IT vendors are now building ERM into their systems. Information technology is critical to ERM, and more organizations are involving the chief information officer (CIO) or another key member of the IT office. For example, at the University of California, the CIO designated a top person to sit on the university's ERM committee.

Management

Management is a broad term that includes the CFO and other senior officers (e.g., chief administrative officer, executive vice president, general counsel) as well as others. While the term "management" duplicates some roles already included in this section, we believe it also warrants a separate mention in this paper.

Collectively, management is responsible for the day-to-day operations of the institution. In ERM terminology, management is responsible for managing the strategic, operational, financial, and compliance risks under the oversight of the president and the board. Management should keep the board informed and consult with the board about risks as appropriate.

Summit participants noted that ERM is simply "good management" and so executing it is clearly management's responsibility. The participants also observed that "line managers" (i.e., department heads, such as the head of the chemistry department, or unit heads like the student financial aid officer) are in the best position to identify risks and to develop ways to mitigate them. As one participant put it, "If line managers don't view ERM as part of their day job, then the initiative will not be successful."

Internal Audit

In the corporate environment, internal audit and risk management are separate and distinct functions. Some ERM Summit participants concluded that a clear separation between the two in higher education may not be needed. In fact, internal audit and risk management may want to collaborate, and at a minimum, they should make sure they are not duplicating tasks. However, it is important to note that internal auditors should by definition be independent and capable of reviewing and reporting to boards if established processes and procedures are followed and working. Several participants noted that if the ERM process is developed and managed by internal audit, they may lose their independence to monitor process

efficiency and effectiveness. Internal auditors can have a supporting role in ERM but a leadership role may compromise their core audit function.

One summit participant indicated that the institution's internal audit director also functions as the chief risk officer. Although it may not be appropriate on many campuses, the arrangement makes sense given the institution and the individual's skill sets. The internal audit director/chief risk officer is developing a "virtual" risk management organization, by asking existing staff in various departments at the institution to also be responsible for risk management. Although this arrangement is the most economical, other institutions may want to have separate, dedicated ERM and internal audit staff who coordinate their efforts.

ACTION AGENDA

Summit participants developed a list of resources that they would find useful in advancing the ERM agenda to the higher education industry as a whole and their campuses specifically:

- An ERM best practice summary and report (similar to NACUBO's Advisory Report on Sarbanes Oxley)
- An annual list of industry risk issues, as well as a "dashboard" to be used to manage and monitor such risks
- A standard ERM template for boards and senior management to use in evaluating risks associated with strategic initiatives
- Identification of example risk areas that could lead to likely cost savings
- ERM tools and templates to be utilized in implementing ERM programs
- ERM training curriculum for university administrators
- A library of ERM reference material
- A case study showing how an institution could apply ERM to existing initiatives
- ERM professional development sessions at annual conferences of higher education associations

In developing the guidance above, consideration should be given to distinguishing between public and private institutions, as well as large or small institutions.

CONCLUSION

The ERM Summit sought to develop a higher-education-specific, sustainable model for ERM and to discuss the appropriate roles and responsibilities for presidents, business officers, risk officers, and trustees.

Clearly, the participants supported ERM for higher education. They took time out of their demanding schedules to attend the summit, and they enthusiastically and thoughtfully contributed to the dialogue with their peers. Most already had an ERM program, about which they willingly shared details with the participants as well as the authors of this paper.

Important findings of the ERM Summit are summarized in Chart 2. But perhaps the most important finding of the summit is that more work needs to be done. The participants suggested that ERM "tools" (e.g., evolving best practice checklist) would be very helpful.

Although risk cannot be eliminated, it can be managed. ERM provides a framework that can enable an institution to manage risk and accomplish its goals. ERM is relevant to all types of organizations, including colleges and universities, and it supports accountability. As COSO says: "Enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way."[7]

Chart 2: Risk Management in Action

Recognizing that higher education's most significant costs relate to labor, look for people-related opportunities (e.g., health and safety) to identify low-hanging fruit for an ERM initiative.

Don't overlook small dollar opportunities. They can add up rapidly and will give the ERM initiative some quick successes.

Incorporate risk management responsibilities into formal individual goals, and build into job descriptions over the longer term. Also, tie meeting ERM goals to compensation.

ERM can help institutions allocate funds from the annual operating budget (and the capital budget) to the most strategic initiatives.

Make contingency plans for high impact/high probability events and for high impact/low-to-medium probability events.

- Consider developing an "adaptable" response that could work for several situations.
- Consider rehearsing possible responses to high probability/high impact situations.

Consider establishing an ERM committee composed of administrators right below the institution's senior officers, who are closest to day-to-day operations and in the best position to identify and manage risks.

Implement ERM in two tracks—one for new initiatives and one for continuing initiatives:

- Begin with strategy for new initiatives and analyze the new initiatives using all eight ERM components.
- Identify enhancements for continuing initiatives by reviewing the eight ERM components.

Communications and training are a crucial component of ERM:

- New and existing employees need to know what's expected.
- Written policies and procedures put expected behavior in writing through written policies and procedures.
- Monitoring activities ensure that employees are doing what's expected.
- When a new initiative is announced, communications and training are needed so that employees can understand how their work fits into the overall strategy.

Faculty buy in is critical to ensure a successful ERM initiative.

Spend time on roles and responsibilities, and discuss them sufficiently for clarity. In general, the:

- board oversees ERM, but leaves the details to management;
- president sets high-level ERM agenda, and engages the faculty and board members in ERM;
- CFO establishes and manages ERM;
- CRO leads ERM and fosters a collaborative, campus-wide approach; and
- internal audit collaborates with CRO.

7 *Enterprise Risk Management—Integrated Framework*, published by COSO in 2004.

ERM Summit Participants

Janice Abraham, United Educators Insurance
Lauren J. Brisky, Vanderbilt University
James S. Broadhurst, Pennsylvania State University
Mary Lee Brown, University of Pennsylvania
Carol N. Campbell, Arizona State University
Grace Crickette, University of California
Ronald G. Ehrenberg, Cornell University
Andrew Evans, Wellesley College
Barbara Feiner, Washington University in St. Louis
Susan Fitzgerald, Moody's Investors Service
Herve Geny, ICAP plc
Karen L. Hendricks, Ohio State University Board of Trustees
F. Robert Huth, Jr., Middlebury College
Louis G. Hutt, Bennett, Hutt & Co.
Jim Hyatt, Virginia Tech
Honorable Jack Jewett, Arizona Board of Regents
Jim Keyes, Middlebury College
Gary W. Langsdale, Pennsylvania State University
Richard D. Legon, Association of Governing Boards of Universities and Colleges
John A. Mattie, PricewaterhouseCoopers, LLP
Deborah Moon, Carnegie Mellon University
Stan Nosek, University of California, Davis
Mark Olson, IBM Global Business Services
Morgan R. Olsen, Purdue University
Yoke San L. Reynolds, University of Virginia
Dorothy K. Robinson, Yale University
Joseph A. Sabatini, Case Western Reserve University
Hossein Sadid, Case Western Reserve University
Carlos Santiago, University of Wisconsin-Milwaukee
Gary C. Schultz, Pennsylvania State University
Patricia Simmons, University of Minnesota Board of Regents
Graham B. Spanier, Pennsylvania State University
Richard R. Spies, Brown University
Thomas E. Spurgeon, Lincoln Office
James Stalder, PricewaterhouseCoopers, LLP
Todd Tueller, IBM Global Business Services
John Walda, National Association of College and University Business Officers
Rick N. Whitfield, Pace University
John O. Wynne, Landmark Communications, Inc.

1133 20th St. N.W., Suite 300
Washington, DC 20036
202-296-8400
www.agb.org

National Association of College and University Business Officers
1110 Vermont Ave., N.W., Suite 800
Washington, DC 20005
202-861-2500
www.nacubo.org