



VICE PRESIDENT—FINANCIAL MANAGEMENT

OFFICE OF THE PRESIDENT
1111 Franklin Street, 10th Floor
Oakland, California 94607-5200

May 15, 2008


VICE CHANCELLORS—ADMINISTRATION
MEDICAL CENTER CHIEF EXECUTIVE OFFICERS

Subject: Enterprise Risk Management at the University of California

On behalf of the ERM Panel, I would like to thank all of you who have moved forward with Enterprise Risk Management. Because of your efforts, eight campuses and two Medical Centers have either formed ERM groups or expanded the scope of existing groups to include ERM, without the “aid” of any particular policy. Campuses and Medical Centers have expressed that they have done so because they see a value in forming these groups and being proactive in managing their risk.

We are pleased to provide for your review and comment the Enterprise Risk Management Report prepared by the ERM Panel. As a leading institution of higher education and financial practices, the University of California adopted the ERM framework advocated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). An ERM Panel was formed that includes management representatives from Office of the President and the campuses (see Appendix C of the report for a listing of Panel members). Moving forward the Panel will include at least one representative from each location.

We hope that the Panel’s report will inspire you to continue moving your programs forward and developing an enterprise-wide approach to managing risk.


Anne C. Broome
Vice President—Finance

Attachment



University of California
Enterprise Risk Management Report to
the Vice Chancellors of Administration
and Medical Center CEOs

presented by the ERM Panel

Introduction

The Enterprise Risk Management panel has prepared this report to update you on our efforts in the past two years and share our ideas for moving forward with advancing enterprise risk management at the University of California.

Why should you be interested in enterprise risk management (ERM)?

- ERM is a best practice. The majority of universities across the US are in the midst of implementing ERM programs. For more information, see the attached white paper in Appendix A: “ERM in Higher Education”.
- Rating agencies are beginning to care about ERM. In November 2007, Standard & Poor’s issued a Request for Comment indicating its intention to assign scores of ERM quality to all companies it reviews and to incorporate an ERM segment into its ratings reports. See Appendix B: “Credit Rating Analysis of Enterprise Risk Management at Nonfinancial Companies: Are You Ready?” for more discussion.
- ERM increases awareness of campus and medical center activities and risks, thereby allowing for better management of those activities.
- ERM provides a common language to communicate, a process to identify and mitigate risks, and criteria to evaluate and prioritize resources, which creates efficiencies.
- It will save the University money.

How does ERM save money? The current total cost of risk analysis identifies over \$220 Million in costs that with a greater consideration of risk can be greatly reduced. We know that the actual cost of risk is much greater and that with ERM we will be able to better understand activities and risks and also to quantify and reduce associated cost. By strategically managing high priority risk we have been able to save over \$180 Million in the last two years.

We also know from managing University claims that had the University gone through the simple exercise of applying the COSO framework during the strategic planning phase of just one single program, the university could have saved over \$18 Million in costs as well as safeguarded our reputation.

We are not suggesting an increase in staff, nor expense, but rather advocating that steps be taken to support the efforts already in place which include:

- supporting existing ERM groups
- supporting key groups that currently monitor and manage risk:
 - Compliance and Internal Audit
 - Controllers and Control & Accountability Directors
 - Environmental Health and Safety
 - Medical Directors
 - Risk Management

We hope that you will take the time to review the remainder of this report and we look forward to your comments.

ERM at the University of California

Since 1996, the University of California has been moving towards an enterprise approach to identifying and managing risk:

- The Regents adopt COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework (1996)
- Controller positions established at each campus and Agricultural and Natural Resources (ANR) (late 1990s)
- Several campuses and ANR develop ERM initiatives (2004–present)
- UCOP Chief Risk Officer position established December 2004
- ERM Panel formed to develop an ERM strategy (June 2005)
- ERM meetings and interviews completed (October 2006)
- ERM survey completed (February 2007)
- ERM Panels formed at most campuses and medical centers (August 2007)
- The Regents appoint Chief Compliance and Audit Officer (October 2007)

As a leading institution of higher education and financial practices, the University of California adopted the ERM framework advocated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). An ERM Panel was formed that includes management representatives from Office of the President and the campuses. Our initial ERM strategy for the UC system was to develop a data warehouse that could manage information that is currently being collected by various groups, existing programs, and initiatives throughout the system. This data could then be analyzed with the COSO framework relative to processes, risks, and controls systemwide. This data warehouse will be an Enterprise Risk Management Information System (ERMIS) and will be implemented in 2008/2009.

ERM meetings, interviews, and surveys were completed to identify key risk factors, key controls, and data already being collected that would be helpful in monitoring our ERM strategic plans and goals.

According to the University Risk Management and Insurance Association (URMIA) and the National Association of College and University Business Officers (NACUBO), many Universities are taking major steps to implement ERM programs. For more information, see the URMIA white paper in Appendix A: “ERM in Higher Education”.

UC’s campuses and medical centers are at varying degrees of implementing ERM initiatives, with eight campuses and two medical centers having already either formed ERM groups or expanded the scope of existing groups to include ERM, without the “aid” of any particular policy. Campuses and medical centers have expressed that they have done so because they see a value in forming these groups and being proactive in managing their risk.

To assist campuses in this effort, the Office of the President Risk Services (OPRS) website provides resources, reference materials, links to helpful websites, and a tool kit of sample forms and documents focused on ERM and Risk Assessment. Additionally, with the development of

the UC Systemwide Ethics and Compliance Program, more resources will become available for assisting with identification, analysis, and mitigation of risks in regulatory and policy compliance.

We have also focused on managing our traditional risk program in a more “enterprising” manner by encouraging a cross discipline approach to managing risk. For example, our Risk Management Leadership Council’s associated workgroups are made up of subject experts rather than Risk Managers. Our Be Smart About Safety program is a collaborative effort rather than a Risk Management or Environment, Health and Safety (EH&S) effort. Our ERM program includes looking at our Total Cost of Risk and by identifying and analyzing the full cost of risk, we have been able to develop strategic plans to reduce the cost of risk and free up resources to be used for meeting the University's mission. ERM also supports the monitoring of internal controls and accountability, providing valuable information to Compliance, the Controllers, and Internal Auditors.

ERM Maturity Models

While there are a variety of frameworks and maturity models for ERM, the Panel, in keeping with the Regents’ adoption of the COSO Framework, have elected to measure our maturity based on COSO:

- Level 0 – Non-existent; there are no planned actions in the area.
- Level 1 – Awareness; management recognizes need for development.
- Level 2 – Developing; component is in planning and development phase.
- Level 3 – Practicing; component exists and is used; however, formal definitions and documentation may not currently exist.
- Level 4 – Optimizing; component is continuously practiced, formal structured definitions and documentation in process.
- Level 5 – Leading; component is accurately defined, documented, communicated, and aligned with ongoing management practices.

The Panel will be developing suggested factors that would indicate levels of maturity.

Steps to Advancing ERM

The COSO framework describes the eight interrelated components of ERM, which are derived from the way management runs an enterprise and integrated with the management process:

1. Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
2. Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

3. Event Identification – Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.
4. Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
5. Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
6. Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
8. Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

The Panel believes that its focus should be on supporting the development and strengthening of the local ERM groups in integrating these eight components into their management processes.

Actions Taken:

- OPRS maintains an online library that includes a toolkit for ERM programs: surveys, assessments, risk mapping, etc.
- OPRS provides ongoing training and plan development with local ERM groups, both at the campuses and medical centers and by presenting Risk Summit sessions focused on ERM.
- UC Systemwide Ethics and Compliance Program is in the process of development and implementation.
- Eight campuses and one medical center have already formed ERM groups or expanded existing groups to include ERM. ANR is establishing a new ERM group to incorporate new senior management.
 - Berkeley – The ERM Initiative Steering Committee has not yet been formalized, but work is already underway. Work to date has focused on identifying risks, risk ownership, and data; future activities include development of comprehensive risk management policy, prioritization of risks, and increased communication with the campus community.
 - Davis – The ERM Group has been active since 2003 and has conducted enterprise risk assessments focused on risks that might prevent Davis from completing its strategic plans. In order to take best advantage of the shared oversight between

them, the campus and medical center are working together to address ERM. The workgroup is made up of representatives from more than a dozen different departments and includes both campus and medical center leadership.

- Irvine – The ERM Council includes members from Materiel & Risk Management, Workers’ Compensation, EH&S, Internal Controls, Internal Audit, and the Controller’s office, and is reviewing membership to determine which other groups should be included (such as Academic Personnel). The Council is evaluating ERM techniques and working on ways to implement ERM into the UCI culture
- Los Angeles – The Controls Work Group was established by the Chancellor to provide oversight to the strengthening and maintenance of Los Angeles’ systems of internal control and accountability. The Controls Work Group meets on a regular basis to monitor campus control systems and to help ensure the deployment of reasonable and understandable policies and procedures across the campus.
- Merced – The Enterprise Risk Management Advisory Committee will advise the Vice Chancellor for Administration by collaborating to identify and manage the full range of risks the University faces. The Committee will champion the resultant strategies and be charged with communicating them to each member’s respective areas. A common language for managing risks will be established with a balanced view – one that attempts to minimize hazards, influence and control uncertainties, and manage opportunities.
- Riverside – The ERM Committee members are a broad array of administrative departments, plus a smattering of others including Office of Research, Health Center, Audit, etc. The current charter is informal, but under development. Campus Strategic Goals, developed commensurate with ERM Objectives and an ERM Survey, is meant to be utilized to assess departments’ alignment with ERM objectives.
- Santa Barbara – The Control Advisory Committee’s focus to date has been financial risk, but the group plans to expand into ERM activities and will discuss ERM at their next meeting.
- San Diego Medical Center – The medical center will expand the scope of its compliance committee and designate it as the Compliance & ERM Committee, rather than having two separate committees with mostly the same members (an expanded roster from the senior management team) as originally planned. The Compliance & ERM Committee will meet quarterly and is planning to conduct a risk assessment based on their new strategic plan.
- San Diego – The Committee on Accountability and Controls has been in existence for over a decade. Its purpose has been to identify issues of concern regarding accountability and controls, but this has evolved to identification, definition and assessment of institutional risk, primarily associated with business issues. The Committee also sponsors an annual self-assessment survey of campus departments regarding risk and control issues. The Committee includes

representatives of faculty, business officers, health sciences, compliance, and all vice chancellor areas. This group is considering moving toward an ERM strategy.

- San Francisco – A Comprehensive Compliance and Internal Controls Committee will hear ERM presentations and discuss how ERM and the committee’s mission may converge once systemwide ERM metrics are better understood.
- An Enterprise Risk Management Information System (ERMIS) is in development and the local ERM panels will have full use of this tool to aid in their risk assessments, monitoring of risk and controls, and producing business intelligence dashboards and reports.

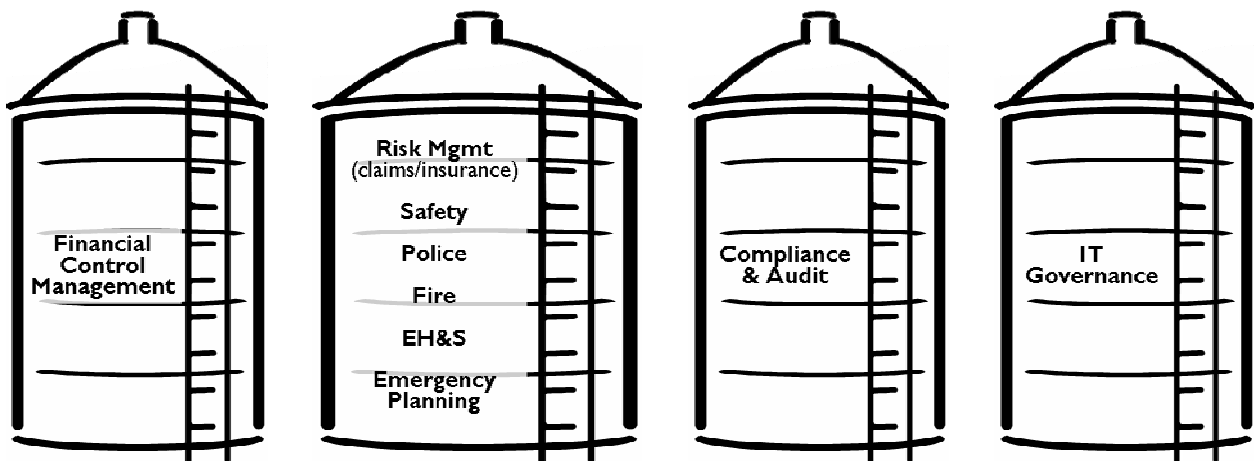
The ERMIS combines a risk management tool, a survey tool, and a reporting tool, all linked to a central relational data warehouse, which will manage new and existing information.

- Risk Management Tool – The risk tool, IBM Workplace for Business Controls and Reporting (WBCR), uses the COSO framework methodology and provides the capability to automate significant aspects of internal control, including control observations and auditor observations. Processes, sub-processes, objectives, risks, controls, procedures, and remediation will reside on this tool.
- Survey Tool – The survey tool is also part of the WBCR. Its functionality includes survey authoring, automatic distribution, response management, and reporting of results. Its question set reusability will eliminate rework by campuses and business areas.
- Reporting Tool – The reporting tool, Cognos 8, includes scorecards, dashboards, multi-dimensional on-line analytical processing (OLAP) cubes, and ad-hoc reports and will be available for all stakeholders, decision makers, and information consumers.
- Currently the following groups are working with IBM to use the system to support and automate their existing programs:
 - Compliance and Internal Audit
 - Controllers and Control & Accountability Directors
 - Environmental Health & Safety
 - Medical Directors
 - Risk Management

Recommended Actions:

- The ERM Panel, OPRS, and other internal and external experts should provide regular and ongoing support to the ERM groups in the way of consultation, training, presentations, and tools.
- Sharing of best practices should be facilitated by OPRS and the ERM Panel.

- All remaining campuses and medical centers should form ERM groups or expand existing groups' scope to include ERM with support and approval from campus administration.
- Also, in keeping with ERM, we would suggest that the consolidation of one or more of the following groups should be considered:
 - Audit Committees
 - Control and Accountability Committees
 - Existing ERM groups
 - Strategic Planning
- In the past, the management of risk has been siloed. This can lead to inefficiencies and redundancies:
 - Multiple assessments
 - Multiple IT systems



Providing an organized approach to gathering business control information including financial reporting, ERM will allow for a timely, comprehensive, consistent, and integrated view of risks, controls, and mitigation across business processes and across the UC campuses. A systemwide central repository for documentation, the ERMIS will spur collaboration and eliminate the need to have separate databases, spreadsheets, and hardcopies of the same information. Stakeholders and decision makers will be able to perform more in-depth analysis and will spend less time identifying, collecting, and aggregating disparate data from the many data sources scattered across the UC system.

The ERM Panel and OPRS look forward to working with the campuses and medical centers on this effort.

For more information, please visit the OPRS website at <http://www.ucop.edu/riskmgt/> or contact Chief Risk Officer Grace Crickette (telephone 510-987-9820, email grace.crickette@ucop.edu).

Appendix A: “ERM in Higher Education”

ERM in Higher Education

September 2007

Sheri Ackley,
University of Wisconsin, System

Megan Adams, Esq.,
Princeton University

Grace M. Crickette,
ARM, CCSA, SPHR, CSHM, RPA
*University of California,
Office of the President*

Christine Eick,
Ed.D., MS, ARM, DRM
Auburn University

Leta Finch, MPA, DRM
*Arthur J. Gallagher Risk Management
Services (Northeast)*

Richard W. Freeman,
Lehigh University

Bonney J. Hebert,
*Academic Risk Resources &
Insurance, LLC*

Gary W. Langsdale, ARM
*Pennsylvania State
University*

Catherine Lark, ARM
Dartmouth College

Ellen M. Shew Holland, ARM
University of Denver

Ruth A. Unks, ARM
*Maricopa County
Community College District*

Editor:
Vincent E. Morris,
CPCU, ARM, AIC, CRM, CIC
Wheaton College

This URMIA White Paper is published by the University Risk Management and Insurance Association (URMIA), P. O. Box 1027, Bloomington, IN 47402-1027. URMIA is an incorporated nonprofit professional organization.

The September 2007 URMIA White Paper was edited by Vincent Morris, Wheaton College, 501 College Avenue, Wheaton, Illinois 60187, layout by Jenny Whittington of URMIA, Bloomington, Indiana, and printed at Regis University Printing Services, Denver, CO 80221.

There is no charge to members for this publication. It is a privilege of membership. Additional copies are available by contacting the URMIA National Office at the address above or at www.urmia.org. Membership information is also available.

© LEGAL NOTICE AND COPYRIGHT: The material herein is copyright September 2007 URMIA; all rights reserved.

Contents

Introduction: A New World of Risk	1
Risk Management Evolution and the New Language of Risk.....	3
What is “risk”?.....	5
How Does ERM Work in Higher Education vs. the Corporate World and Why Should I Care?	7
ERM Frameworks	9
Developing an ERM Framework of Your Own	15
Elevating Awareness of Enterprise Risk Management in Institutions of Higher Education	17
Conclusion: The Secrets to Success.....	21
Appendix A—How to Make It Work: ERM at Auburn	23
Appendix B—How to Make It Work: ERM at Penn State	25
Appendix C—How to Make It Work: ERM at Maricopa County Community College District.....	27
Appendix D—How to Make It Work: ERM at University of California	31
Suggested Tools, References, and Resources for More Information	37
Glossary of Common Terms Associated with Enterprise Risk Management	41
Bibliography	46

Introduction: A New World of Risk

After devastating accounting scandals rocked the U. S. at the turn of the millennium, increased levels of regulatory compliance were promulgated as a result of the Public Company Accounting Reform and Investor Protection Act of 2002 (also known as the Sarbanes-Oxley Act, Sarbox, or simply SOX). SOX, along with other regulatory compliance events and regulations, sent many corporations in the United States scrambling toward a new level of risk management. While SOX compliance is only required for publicly traded organizations, many have chosen to do so voluntarily—some in anticipation of being required to comply in the future; others believing that such compliance represents a best practice in risk management. These institutions are working with their boards of trustees toward a more efficient management of institutional resources through the discipline of Enterprise Risk Management (ERM).

With this new world of risk in mind, the University Risk Management and Insurance Association (URMIA) appointed a task force of risk managers and authors who have worked together to prepare this White Paper on Enterprise Risk Management, to provide URMIA members and institutional colleagues with both a better general understanding of this management process, and also a set of resources on how to implement the ERM process.

Note that this document will not give a detailed, step-by-step guide on how to implement ERM at any specific institution. However, it will provide a good overview of the process, where to begin, and best resources available for structuring and implementing an ERM framework.

Toward that end, and perhaps most helpful in this document, are the Appendices describing how other schools have implemented ERM. We especially thank Grace Crickette of the University of California, Office of the President, Dr. Christine Eick of Auburn University, Gary Langsdale of Pennsylvania State University, and Ruth Unks of Maricopa County Community College District for their willingness to share their programs, “warts and all.”

Risk Management Evolution and the New Language of Risk

The practice of Risk Management as a discipline has been changing steadily for the last twenty years and especially in the last five. URMIA is particularly interested in advancements in the risk management field and is the key source for higher education risk management information. Other organizations that educate and track risk management trends are the Association of College and University Auditors (ACUA) and the Public Risk Management Association (PRIMA), which has recognized that the transformation of risk management includes organizational vision, mission and strategies.

Another important higher education business organization is the National Association of College and University Business Officers (NACUBO), which noted in a 2000 publication the advent of the most recent changes in risk management:

Risk management evolved from insurance buying when methods other than insurance buying began to be used to treat risk exposures. Originally the scope of risk management was narrowly defined to include only accidents that resulted in a loss. In the 1980s, as sophisticated risk financing became an important alternative to insurance, risk management expanded to include other risk transfer and risk control strategies. Now the evolution continues as the focus of traditional risk management expands into strategic risk management, an even more comprehensive approach that does include investment, business, and political risks.

Each of these organizations are developing various aspects of ERM for implementation in higher education settings. As these ERM pathways converge, sometimes in confusing ways, a brief review of the history of ERM developments may be helpful.

In the late 1980s, long before SOX, several significant business failures occurred as a result of high-risk financing strategies. These events and their negative outcomes resulted in authoritative standard-setting bodies for the financial services, accounting, and auditing industries to convene and assess the nature of the business failures. The result was the commissioning of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), sponsored and funded by the American Institute of Certified Public Accountants (AICPA), the American Accounting Association (AAA), the Financial Executives Institute (FEI), the Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). COSO was charged with conducting a study of the business failures and issuing guidance on how to prevent reoccurrences. The outcome of COSO's review of internal control systems was the recognition and communication of the need for managing organizations to shift from strictly a financial focus to a focus on managing "business risks."

The COSO report provided a common language regarding controls, and created an integrated control framework for managing business risks. The framework consists of five interrelated components: 1) control environment, 2) risk assessment, 3) control activities, 4) information and communication, and 5) monitoring.

The *control environment* component is considered the “framework.” It focuses on people, the ethical and moral values established by an organization’s leadership team, and competence. It emphasizes that people *are* the organization and are the key determinants of the organization’s success or failure.

The *risk assessment* component ensures that mechanisms exist throughout the organization to identify, manage, and mitigate unwarranted risks. Therefore, goal alignment is critical throughout the organization and is to be integrated throughout all significant activities.

The *control activities* component provides that policies and procedures should be established and followed to ensure all actions support the achievement of defined goals.

The *information and communication* component provides that communication and the sharing of information should occur up, down, and across the organization. It requires that information be timely and thorough in order for actions to be completed that support the achievement of stated goals.

The *monitoring* component provides that the entire process must be monitored in order to recognize problems to make necessary adjustments during the course of operations.

What is “risk”?

Before risks can be effectively managed, an organization must agree on a common definition of risk that is clearly understood throughout the organization by the board, management, and staff. The 2001 NACUBO publication *Developing A Strategy to Manage Enterprisewide Risk in Higher Education* defines risk as “any issue that impacts an organization’s ability to meet its objectives. Five types of risk include: strategic, financial, operational, compliance, and reputational.”

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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The consultancy group Tillinghast-Towers Perrin defines ERM as “a rigorous approach to assessing and addressing the risks from all sources that threaten the achievement of an organization’s strategic objectives. In addition, ERM identifies those risks that represent corresponding opportunities to exploit for competitive advantage.”

As the corporate world wrestles with new and broader definitions of risk, ERM has become the common currency of the risk management discipline and is beginning to provide the primary vocabulary as well.

How Does ERM Work in Higher Education vs. the Corporate World—and Why Should I Care?

As higher-education leaders develop business strategies for the 21st century, it is important to recognize and continuously examine the market forces changing not only our society, but also the entire economy and related business environments that envelop our complex higher education institutions. This is a key purpose of an ERM framework.

The following drivers are increasing pressure to transform higher education:

- Fierce competition for faculty, students, staff, and financial resources.
- Pressure for increased productivity, responsiveness, and accountability while reducing costs.
- Increased external scrutiny from government, the public, governing boards, journalists, and taxpayers'-rights groups.
- Powerful new technologies that require significant investment of both financial and human capital resources.
- Rapidly increasing entrepreneurial ventures beyond the traditional educational venues that create stresses and strains on traditional administrative and financial infrastructures.
- Increased competition in the marketplace.
- Increased levels of litigation in general and internally, with ever-increasing levels of financial consequences.

As higher education leaders map new strategies to address these drivers, it is especially important to note that *business* risks have increased. Leaders understand these risks, and they establish a “risk conscious” tone at the top for their organizations. These business risk areas include:

- **Strategic Risks—Goals of the Organization:** In developing strategic plans, colleges and universities should consider the risks associated with each strategy. Institutions of higher learning must market their unique advantages, strive to be competitive and be a vital presence in the communities they serve. An appropriate ERM framework should support the upside of risk (benefits) and protect against the downside of risks in all these endeavors.
- **Operational Risks—Processes that Achieve Goals:** Colleges and universities are dependent upon day-to-day operations for their success and, as such, must assess operational risks.
- **Financial Risks—Safeguarding Assets:** Finance divisions, including risk management departments, traditionally have focused on managing the risks of potential loss of physical assets and financial resources.

- **Compliance Risks—Laws and Regulations:** This area includes internal and external reporting and may involve financial and non-financial information. Non-compliance with external laws, regulations and rules can be costly. Some of the most significant penalties have come from ineffective management of compliance risks.
- **Reputational Risks—Public Image:** Many organizations' images have been damaged and reputations tarnished by failure to effectively manage reputational risks. Emphasis on employee and educational integrity and a clear statement of the ethics and moral values emanating from the top is an important component of this risk.

Enterprise Risk Management links institutional governance, risk management, and the strategic goals of the institution. Simply put, it is a way to more effectively manage *all* of the risks that exist on a college or university campus. The financial benefits of ERM for a school can include:

- Cost-effective management all of its resources
- Greater efficiencies in use of constrained resources
- Maintaining competitive advantages, resulting in enhanced use of existing applications
- Eliminating paying fines for regulatory non-compliance
- Enhanced capital and reduced loss of assets
- Reduced cost of turnover by avoiding employment liability exposures
- Reduced legal expenses
- Enhanced communications across departmental “silos,” the self-contained management of risk without reference to the overall goals and strategy of the organization)
- Reduced claims or operational losses by enhanced loss prevention.

ERM helps an institution to:

- Sustain its competitive advantage
- Solidify its integrity and reputation
- Respond effectively when a significant event occurs
- Avoid financial surprises
- Effectively manage all of its resources

Instead of having only a few personnel dedicated to managing traditional risks on campus, ERM engages everyone at the institution in the management of those risks for which they are responsible.

ERM Frameworks

The first step in implementing ERM is to establish a *framework*. This is the overarching structure under which reside the basic components that make up enterprise risk management. Each institution's framework will be unique. It is through the building of a framework that each organization decides which ERM components best address needs and then decides how these components will be implemented on campus. These choices will be influenced by the institution's goals, objectives, risk management culture and philosophy.

The ERM framework incorporates the organization's ERM goals and objectives, management oversight, written plan, processes, tools and methods for full implementation across the university. It also incorporates a systematic approach to evaluating and improving the effectiveness of the ERM program.

It is important to establish from the beginning what the *objectives* of the ERM framework will be. For example, the University of Regina's (SK, Canada) policy on ERM describes the objective of their framework as follows:

“ERM, through the application of the framework objectives, aids in the achievement of the University strategic priorities and advances the management practices at the University. Specifically, the ERM framework objectives are to:

- a. Incorporate a consistent approach to risk management into the culture and strategic planning processes of the University, supporting the setting of priorities and making of decisions at the institutional level, as well as at the operational and administrative unit levels.
- b. Apply a consistent approach to risk response and control activities to support the University's governance responsibilities for innovation and responsible risk-taking, policy development, programs and objectives. In all cases, appropriate measures will be put in place to address unfavorable impacts from risks and favorable benefits from opportunities.
- c. Manage a transparent approach to risk through formal and informal communication and monitoring of all key risks, balancing the cost of managing the risk with the anticipated benefit. Risk management practices will be adapted to encompass best practices, specific circumstances and mandate.”

These framework objectives exemplify the starting point in the development of a comprehensive ERM program that embodies the intent of COSO, as well as other widely accepted ERM approaches.

Framework Options

In determining how to develop their own specific institutional ERM framework, higher education administrators may wish to familiarize themselves with the various ERM framework approaches that have been published by professional organizations, largely in the U. S. but also in the United Kingdom, Australia, New Zealand and Canada. Some of these frameworks come from engineering, accounting and auditing organizations, while others come from the insurance industry. The different backgrounds lead to very different approaches. Some, for example, lead specifically towards financial reporting.

Examples of major existing frameworks are:

- 1) COSO's *Enterprise Risk Management—Integrated Framework*
- 2) Australia/New Zealand Standard—*Risk Management*
- 3) ISO Risk Management—*Draft Standard*
- 4) The Combined Code and Turnbull Guidance
- 5) *A Risk Management Standard* by the Federation of European Risk Management Associations (FERMA)

Three of these frameworks, in particular, seem to be most suitable for use by colleges and universities. They can be summarized as follows:

1. COSO's *Enterprise Risk Management—Integrated Framework*

In 2004, COSO published a document entitled *Enterprise Risk Management—Integrated Framework* with the objective of “providing an ERM framework, key principles and concepts, a common language, and clear direction and guidance” for companies wishing to consider implementing, evaluating and improving ERM programs. COSO distinguishes this publication from the 1992 COSO publication entitled *Internal Control—Integrated Framework*, which continues to serve “as the broadly accepted standard for satisfying” Sarbanes-Oxley 404 requirements. The 2004 publication “expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management” and “does not replace the internal control framework but rather incorporates the internal control framework within it.”

The COSO ERM framework can be depicted as a three-dimensional matrix (Exhibit 1). The top side of the matrix sets forth the four major categories of ERM program objectives. The front face of the matrix shows the eight interrelated components of an ERM program. The COSO publication discusses each of these components in detail. These components are the mechanisms and processes by which ERM program objectives are achieved. The third dimension simply indicates that ERM is intended to be implemented on an organization-wide basis.

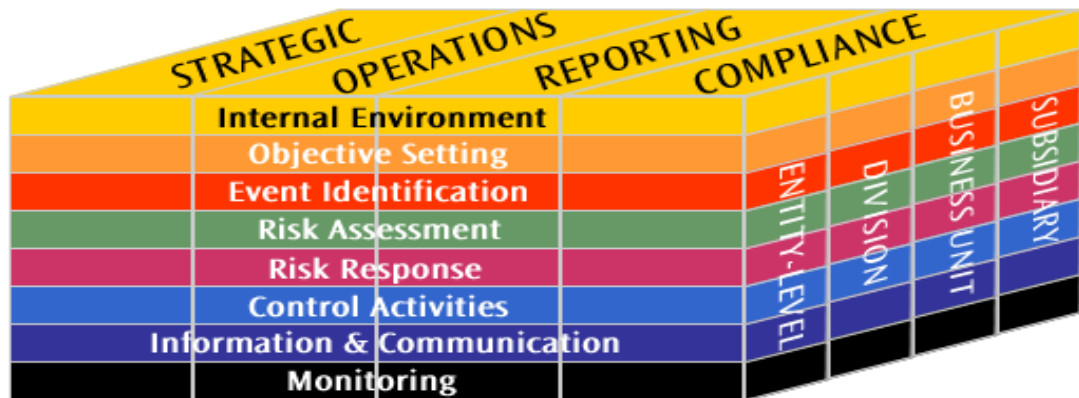


EXHIBIT 1

© 1992 by the Committee of Sponsoring Organizations of the Treadway Commission. Reproduced with permission from the AICPA acting as authorized copyright administrator for COSO.

The Executive Summary of the COSO ERM framework can be obtained at www.coso.org. Bound and electronic copies of the complete integrated framework may also be ordered through the website. This document includes the Executive Summary, the Framework and the accompanying Application Techniques, “which provide illustrations of techniques useful in applying elements of the framework.”

2. Australia/New Zealand Standard (AS/NZS 4360:2004)—*Risk Management*

Australia and New Zealand formed a joint technical committee composed of representatives from numerous organizations (profit-making and nonprofit), professional disciplines, and industry sectors to publish two documents on risk management. The first document is the actual *Risk Management Standard*, initially published in 1999. The Standard has been revised and was republished in 2004 as AS/NZS 4360:2004. The second document, entitled *Risk Management Guidelines* (Companion to AS/NZS 4360:2004) provides generic guidance for developing and implementing an effective enterprise-wide risk management process.

The Standard can be adapted for use in any type of organization and for any project. In keeping with current ERM concepts, it attempts to factor in both the upside and downside of risk. An organization that practices ERM will be working diligently to identify risks, manage them and monitor their status. The organization will have a corporate understanding of the types and limits of risk and the amount of overall risk it will tolerate. An effective ERM program will have a management structure and process in place to ensure that losses that occur will be within those tolerances. When an ERM program is effective, the organization will *know* what risks it faces; it will *understand* those risks and understand how to *manage* them. At that point, decision makers will be able to make informed decisions on a risk vs. reward basis. The result of ERM, therefore, fosters a culture of “risk adjusted decision making” and a controlled risk-taking environment. Stakeholders and decision makers can then confront risk with the knowledge that losses are probable but manageable within predetermined limits.

The Standard contains nine steps necessary for creating an effective program:

1. Ensure support of senior management
2. Develop risk management policy
3. Communicate policy
4. Establish accountability and authority
5. Customize the risk management process
6. Identify and provide resources
7. Develop a plan for appropriate organizational levels
8. Manage risks at the area, project and team levels
9. Monitor and review

The *Guidelines* document (Companion to AS/NZS 4360:2004) takes each element of the risk management process (see Exhibit 2) and elaborates on that step. The process itself is very similar to the traditional risk assessment process: identify risks, analyze risks, evaluate risks, treat risks, and monitor and review. A thorough treatment of two additional steps is also incorporated: “Communication and Consultation” and “Establishing the Context.” “Communication and consultation are important considerations at each step of the risk management process. They should

involve a dialogue with stakeholders with efforts focused on consultation rather than a one way flow of information from the decision maker to other stakeholders.” The step “Establishing the Context” focuses on “defining the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process.”

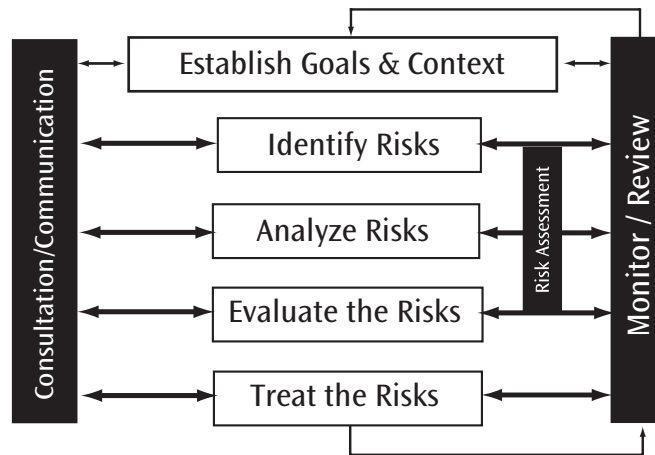


EXHIBIT 2

AS/NZS 4360:2004 Fig 2.1 Reproduced with permission under SAI Global Copyright Licence 0709-c035.

An electronic or hard copy of the complete Standard and companion document can be ordered at <http://www.riskmanagement.com.au/>.

3. ISO Risk Management—*Draft Standard*

The International Organization for Standardization (ISO) is a worldwide federation of national standard-making bodies. ISO is currently developing an ISO Risk Management Standard. This framework is very similar to the Risk Management Process contained in the Australia/New Zealand Standard (2004). As described by ISO, “This International Standard provides generic principles and guidelines for the effective implementation of risk management and is applicable to any organization, regardless of its size and type. It also seeks to assist in the harmonization of risk management processes and definitions in existing and future standards.”

It appears that the final ISO Framework will contain a thorough risk assessment process similar to the one described in the Australia/New Zealand Standard and will be familiar to those who have been practicing traditional risk management.

Developing an ERM Framework of Your Own

It is one thing to know about the best ERM framework-building structures available; another to select one. The basic components of most widely recognized frameworks are similar, with differences mainly in the language used to describe the process and in the number of steps. The trick is to successfully bridge the gap between the general frameworks and become institutionally specific. Every college and university has its own culture, management philosophy, capabilities and needs. Each institution will need to develop or tailor an existing ERM framework to serve their purposes, including defining and employing its own ERM language.

Some schools appoint a Chief Risk Officer (CRO) to oversee the implementation of ERM. A Chief Risk Officer is different from a Risk Manager to the degree that he or she is able to encourage and facilitate the *entire organization* to integrate thinking about the costs *and benefits* of taking risks, and how to manage them, throughout the entire strategic planning process. The Risk Manager may guide or even direct the process, because good risk management already means working with multiple departments, taking a broad view of processes, and analyzing risk. But the Risk Manager will not always be the captain of the ERM ship, as sometimes departments will merge, cross-disciplinary risk committees will form, and other skill sets are employed.

Certainly the leadership attributes for the Chief Risk Officer may be different from those typically sought for a Risk Manager. The CRO will need not only an understanding of insurance, but familiarity with other areas such as Environmental Health and Safety, Security, Facilities Management, Operations, and the Academy. Insurance will always be an important tool in the risk management box, but ERM drives everyone to be more strategic, imaginative, broader, and longer-term risk management solutions.

The essential components of most ERM frameworks are similar. Mature framework models have basic components that bond-rating agencies, auditing firms, accounting firms and risk managers consider necessary for building a credible, workable ERM Framework. They include:

- 1) Goals and Objectives, including the university's rationale for managing risk
- 2) Description of the risk management culture
- 3) Oversight and management structure for ERM infrastructure
- 4) Development of a written plan of implementation
- 5) Risk Management Process (identification, analysis, evaluation, treatment, monitoring)
- 6) Risk reporting
- 7) Communication

As you decide how to implement ERM within your organization, you may want to adapt a generic framework to meet your needs and available resources. The framework depicted in Exhibit 3 contains the essential components of several widely accepted ERM frameworks, compiled and portrayed in a comprehensive generic model.

Exhibit 3: Model Risk Management Framework

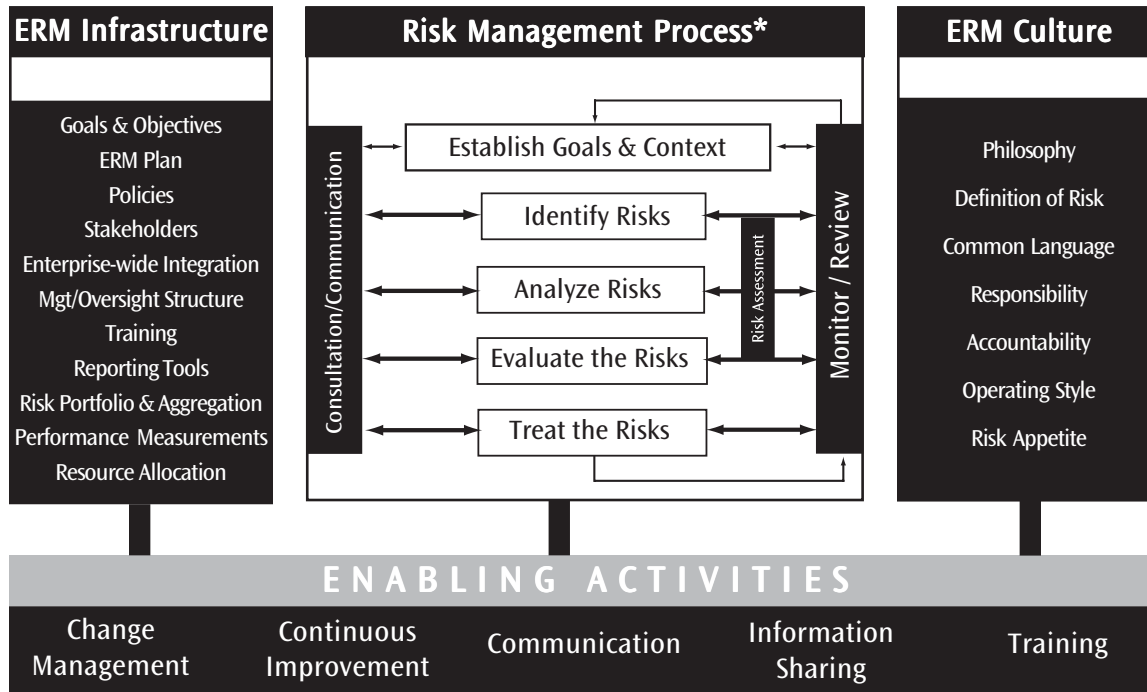


EXHIBIT 3

*Risk Management Process, AS/NZS 4360:2004 Fig 2.1 Reproduced with permission under SAI Global Copyright Licence 0709-c035.

At the core of this framework is the Risk Management Process, which is similar to the standard risk assessment process familiar to many risk management practitioners since its creation in 1972 by Dr. George L. Head (Ph. D., CPCU, ARM, CSP, CLU, Director Emeritus of the Insurance Institutes of America; Dr. Head continues to write and advise on risk management matters). However, the scope and application of the framework is enterprise-wide. Within ERM principles, traditional risk management practices must now be integrated with existing management practices and the supporting enabling activities which have been adopted at your University. In addition, the contemporary concept of ERM goes beyond risk assessment and the traditional goals of protecting assets and mitigation. It embraces the concept of adding value to the organization and *enhancing*, as well as *protecting*, both tangible and intangible assets.

Once you have your ERM framework, the approach and course you will take to implement it can be boiled down to an ERM plan that will keep you on the right path and headed in the right direction.

Elevating Awareness of Enterprise Risk Management in Institutions of Higher Education

It is fine to learn about ERM as applied in the corporate setting, and about the framework options available for tailoring a plan to a specific organization. But you may have questions remaining about how the ERM process works at colleges and universities. Here are a few of the most likely questions and answers:

1. Is ERM really applicable to higher education?

Yes, the ERM process is directly applicable to institutes of higher education, just as it is to any other “enterprise.” Risks are taken, considering both down-side and up-side potential, to minimize loss and maximize competitive advantage. There is nothing so unique to the college or university setting as to make ERM irrelevant or impossible to implement. Since risk management already takes place at the vast majority of schools, ERM simply expands that process up (with the support of the Board and administrators) and across (posing questions about specific risks and management techniques) to all other departments and divisions of the institution.

2. Within the institution, who already may have heard about ERM?

The topic now receives a fair amount of space in the business trade press for financial leaders. It is also being discussed by the credit rating agencies (Moody’s, Standard and Poor’s, Fitch Ratings) in their briefings; for the financial and energy sectors, these rating agencies have already formally incorporated ERM into their analysis of entities under review. NACUBO published a White Paper on the topic of ERM in 2000, and is considering an update.

Based on these indicators, it is safe to say that most Chief Financial Officers, Business Officers and Controllers have probably heard or read about ERM. The Association of Governing Boards has also demonstrated an interest in the topic, including recent articles in their periodical, so Trustees may have heard of it. Further, to the extent that Trustees have other roles in the community such as business leadership, their own companies may have already implemented an ERM program.

PricewaterhouseCoopers has been active in advising Internal Auditors about the COSO model (which PwC authored), and PwC (along with other major accounting firms) offers consulting services on the topic, as do the major insurance brokerages.

Internal Auditors have long used the COSO model in their assessment of risk. External audit firms such as PricewaterhouseCoopers have been very active in promoting the use of the COSO model through various publications. Most external audit firms offer consulting services with respect to ERM, as do the major insurance brokers.

3. Who is likely to be interested?

Within an institution of higher education's management, the board of trustees, the president, the Chief Financial Officer, Controller, Internal Auditor, General Counsel and the Risk Manager. Those persons responsible for developing and monitoring the school's long-term strategic planning efforts will also be interested since ERM may have an impact on the success of the plan. Various other campus departments may also be interested, such as academic affairs, student affairs, athletics, student health, fleet/transportation offices, international education, human resources, police/security, etc.

4. Although the process of earning "buy-in" will differ by institution, what are the basic steps?

If one accepts the idea that the risk management function at an institution of higher education is responsible for evaluating risk issues and working in concert with other responsible parties to deal with those risks, ERM is a value to be incorporated into the decision-making processes. Thus *it is not a distinct product*, but rather it seeks to enhance judgment and decision-making throughout the organization, in such a way as to beg the question "have you thought of...?" when making decisions about any aspect of the enterprise, to be exercised by everyone from the custodial staff to the President. All individuals must "own" the risks their actions encounter, and this ownership will not be supplanted by the implementation of ERM. Therefore, obtaining acceptance of ERM is no different from educating the leaders and staff about any other aspect of improving their productivity or decision-making process. The basic steps include:

- a) Raising awareness of the concept;
- b) Understanding and explaining the growing body of reference material and background information (see question #2 above) about ERM within the higher education sphere;
- c) Explaining how ERM can benefit the leaderships' efforts with a more thoughtful assessment of risk *before* decisions are implemented.
- d) Asking leaders the question, "What keeps you awake at night?" Consideration of this question might spur a dialog that will raise awareness that they can make a difference by consciously incorporating risk issues into their decision-making process. This is the most critical practical piece of ERM. Unless and until each departmental group is actively incorporating "what if?" risk management questions into their long-range planning and decision-making, ERM is not yet a complete reality on campus.

Once leaders understand the basic risk management cycle (identify the risk, quantify the exposure's probability and severity, select and implement treatment, monitor the effects), they can incorporate this into their own processes as formally or informally as the institution may choose. This is the time to introduce basic tools of risk identification and analysis, and assist them in using them to

think about both the costs and the benefits of the risks of their action (or inaction, as the case may be—one of the more exciting aspects of ERM is the seizing of opportunities otherwise passed by because, upon further ERM-level deliberation, the risks seem manageable after all).

ERM can also open the door for a strengthened working partnership between the Risk Manager and the Internal Auditor, since the Internal Auditor has a responsibility to report that appropriate management controls are in place. ERM provides another way for the Audit function to determine that due diligence is done throughout the organization. However, because the Auditor's role is to *evaluate and report* on systems and controls, it is inappropriate for the Auditor to *manage* the systems and controls—but Internal Audit can be an advocate and partner, helping the Risk Manager to explain the benefits of ERM.

Conclusion: The Secrets to Success

Risk Management is not a new discipline. It is not even new to higher education. But the breadth of ideas suggested by *Enterprise Risk Management* is new to both the corporate world and to higher education.

A cookbook recipe for implementing ERM is not feasible, because so much depends on the culture of the organization and the change agents who lead the effort. Success will require the institution's governing board, chief executive officer, and senior management to establish a tone of importance for the initiative, specifying it to be a sustaining approach to managing the institution's resources. Champions of the initiative need to include college administrators, as well as deans, department chairs, and their business administrators. An institution's culture, including existing silo approaches to key activities and well-protected turfs will present barriers to successful implementation. There are a few standard keys to success.

The International Internal Auditors Foundation and the Tillinghast-Towers Perrin report identified six components that are present in successful ERM programs:

- Obtaining strong, visible support from senior management and/or the Board of Directors
- Dedicating a cross-functional group to drive the implementation and continue to push it in its operational phase
- Closely linking ERM to key strategic/financial objectives and to the business planning process
- Introducing ERM as an enhancement to well-accepted processes—not a stand-alone process
- Importing ideas from the outside
- Proceeding incrementally and leveraging “early wins”

According to other ERM literature, in order to attain the highest probability of success in implementing ERM, the following must be present:

- Top-level support, commitment and participation;
- Adequate breadth and depth for participation within the organization;
- An understanding that ERM is a continuous process, not a one-time event;
- An institutionalization of the process of risk assessment, so that the entire institution becomes involved and has ownership of the outcomes.

Organizations that have invested the time and effort to get these fundamentals right have been more satisfied than their peers with the progress of their ERM implementation efforts. They have succeeded because they have laid a clear track to follow, established realistic expectations, assigned clear unambiguous roles and responsibilities, equipped themselves appropriately, and identified objective benchmarks to monitor their progress.

Higher education risk managers who implement this new type of risk management program will elevate their institutions into the elite group of schools who are working to break down the limitations of the “silo approach” to managing risk by integrating traditional risk management and ERM.

Appendix A—How to Make It Work: ERM at Auburn

Auburn University (by Dr. Christine Eick, Executive Director of Risk Management and Safety)

- Total Student Population: 23,547 FTE
- Undergraduate Students: 19,367 FTE
- Graduate Students: 3,245 FTE
- Professional Program Students: 935 FTE
- Employees: 9,450 FTE
- Net Assignable Square Footage: 7,575,927
- Total Revenues: \$575,774,630 (2003)
- Total Organized Research Funds: \$105,108, 747 (2001)

Auburn University, a premier public land-grant research institution located in east Alabama, has a proud and dynamic 150-year history with a strong commitment to instruction, research, and outreach. For Auburn, Enterprise Risk Management means that risk management is part of the university culture and is incorporated into the strategic planning process and goals of every department. Individual departments and divisions at the university will know what their risks are, will take responsibility for managing those risks, and will measure their performance in managing their risks. The key change for us from “typical” risk management is that with ERM, the departments are taking the responsibility for managing their risks through their strategic planning process and are holding themselves accountable for their risk management performance.

I became interested in ERM in the late 1990s, when the risk management and insurance industry began to take a serious look at how we were defining risk management. I saw how risk management evolved from an insurance purchasing function, to an insurance management function, to a broader risk management function. I saw enterprise risk management as the next phase for risk management in its evolution. As a risk management professional I want to stay abreast of what is going on in my field, so I read anything I could find on enterprise risk management. I attended an Advanced Management Program on Enterprise Risk Management, and through that program was introduced to several models that had been successfully implemented in the corporate world. I was surprised, after meeting the Chief Risk Officer for Wal-Mart, to see how well the Wal-Mart model could work in a university setting. Wal-Mart has separate divisions that work very autonomously, in a way that is very similar to how a university has colleges, divisions, and departments that operate in a decentralized fashion.

At the same time, our Executive Director of Internal Auditing was also learning more about enterprise risk management and had a great interest in implementing ERM at Auburn University. He had learned about a method other schools were using that was very similar to the one implemented by the CRO of Wal-Mart and that coincidentally used some of the same tools. The Executive Director of Internal Auditing and I had talked informally about what we were reading and learning about

ERM, and decided that we were ready to bring together what we had learned and create a model system for implementing ERM at Auburn University.

Risk Management and Safety and Internal Auditing were positioned well to begin an ERM program. We both report to high levels in the organization and operate with a fair amount of autonomy. I report to the Executive Vice President and President, and the Executive Director of Internal Auditing reports to the chair of the Board of Trustees Audit Committee. Both of our departments are seen as resources for our university and enjoy positive relationships with Deans, Vice Presidents, and other senior administrators. We also had a common vision for creating an environment where risk management is considered in the strategic planning of every department at Auburn University. We saw that by working together we could pool our contacts and resources to implement ERM.

To help the “risk owners” analyze the risks facing them, we use both an anonymous voting system called Resolver Ballot and the Microsoft Excel spreadsheet program in our risk assessment workshops. We hold the workshops in a “smart classroom” and are able to project the spreadsheets and the Resolver screens, which enables the participants to take an active role in the workshop. We purchased five licenses for the Resolver Ballot software, a receiver for a laptop computer, and twenty-five remote voting pads that are used by the workshop participants in casting their votes. The Resolver Ballot software is loaded with the risks that the workshop participants have identified as their risks. The participants vote on the rankings for the risks using the remote voting pads. The risks are ranked on a scale of 1–5 for 1) the impact the risk has on their organization, 2) the likelihood that the risk will occur, and 3) the degree of influence they have over the risk. The Resolver Ballot program allows for immediate results and is a very efficient tool to use. The data is easily downloaded into Excel, which makes it easy to share the raw data with others who do not have the Resolver software. The Resolver licenses and equipment were under \$15,000.

Appendix B—How to Make It Work: ERM at Penn State

The Pennsylvania State University (by Gary Langsdale, University Risk Officer)

- Total Student Population: 76,387 FTE at 20 campuses
- Undergraduate Students: 68,095 FTE at 17 campuses
- Graduate Students: 8,292 FTE
- Professional Program Students: 1,258 FTE
- Employees: 22,478 FTE at 20 campuses
- Net Assignable Square Footage: 8,060,000 at Main Campus
- Total Revenues: \$3,411,528,000 (2006–07)
- Total Organized Research Funds: \$700,000,000

Penn State is a multi-campus, public land-grant university (publicly supported, but not owned by the State) that improves the lives of the people of Pennsylvania, the nation, and the world through integrated, high-quality programs in teaching, research, and service. Our instructional mission includes undergraduate, graduate, and continuing and distance education informed by scholarship and research. Our research, scholarship, and creative activities promote human and economic development through the expansion of knowledge and its applications in the natural and applied sciences, social sciences, arts, humanities, and the professions.

The goal of Penn State University's ERM program is to provide tools for its leaders and managers to make better risk-adjusted decisions. Those who own the risks need to better understand how they can seamlessly incorporate ERM into their decision-making process so that they can keep risks within the University's tolerance and perhaps gain a competitive advantage.

Investigation of ERM was actually driven by the senior financial leadership of the University, who had read and heard about it from various sources and decided to investigate further. When the University Risk Officer and the Director of Internal Audit were each hired in 2003, they were given the charge by the Senior Vice President of Finance and Business and the Corporate Controller to work together to investigate ERM and determine whether it might be included in the University's work processes. Shortly thereafter, the Finance and Business organization implemented its 2004–2008 Strategic Plan, and ERM was listed as a Key Initiative of that Plan.

The Key Initiative Team has led the way in determining the ERM efforts. As of August 2007, there is not a formal structure to the implementation of ERM beyond the team members' activities, although training for managers is under active development. Keeping in mind that since Penn State University's vision of ERM is *not* to impose any particular structure, but rather to provide tools for use by leaders and managers throughout the University, our activities have focused upon identification of risks, engaging in dialog with the "risk owners," and developing training material.

To date we've stuck with low-tech solutions. The Internal Audit Director and University Risk Officer traveled to all campuses to visit every Chancellor, Dean and senior business unit leader. From that tour came a distinct list of risks, which the Key Initiative Team plugged into a risk map (frequency on one axis, severity on the other) and then prioritized the dozen highest frequency and/or severity risks which could be dealt with, for initial focus. Teams of two team members are now meeting with each of the "risk owners" to ask whether these risks are worthy of consideration, whether further resources are required to manage the risks within the University's tolerance, and whether the "risk owner" is satisfied with the current efforts to manage the risk. Training classes are under active development in conjunction with the University's Human Resource Development office.

To initiate the process, we engaged a consultant to act as facilitator for the Key Initiative Team. This has been a successful strategy, which brought a discipline to the usual group dynamics. Within the University we were quite surprised as the initiative got underway that there was no perceptible resistance to evaluating risks in an ERM format. In the interview process described above, half an hour was allocated for each interview; not a single one went less than a full hour, and many extended to two hours. The leaders expressed sincere interest in discussing their perception of the risks faced by the University, and seemed genuinely appreciative of the effort to work on managing them. We have been pleasantly surprised with the lack of resistance to the concept of ERM. Of course, we haven't really forced anyone to do anything!

Time management is a concern. Because this has been implemented on a project basis, with volunteers pulled from a variety of disciplines across the University, each with their plates already full-to-overflowing (including the project leader!), things have moved more slowly than I would have liked and definitely slower than our Senior VP would prefer. However, he has been patient and is pleased that we are moving forward.

Appendix C—How to Make It Work: ERM at Maricopa County Community College District

Maricopa County Community College District (by Ruth Unks, Risk Manager)

- Total Student Population: 220,085 (FTSE 69,582)
- Undergraduate Students: 220,085
- Employees: 10,000+
- Net Assignable Square Footage: 4,837,650
- Total Revenues: \$649,159,983

The Maricopa Community Colleges comprise ten public colleges, two skill centers and numerous education centers dedicated to educational excellence, meeting the needs of businesses and the citizens of Maricopa County. Each college is individually accredited, yet part of a larger system—the Maricopa County Community College District. The District is one of the largest higher education systems in the world and the largest provider of health care workers and job training in Arizona—a major resource for business and industry and for individuals seeking education and job training.

In November 1999, Dr. Rufus Gasper, Maricopa County Community College District (MCCCD) Chancellor, created a task force to identify the District's top risks. The task force identified 80 risks and prioritized them. In March 2000, the MCCCD Governing Board approved a project designed to assess these risks. In October 2003, Chancellor Gasper merged the enterprise risk management committee and the Risk Management Advisory Committee to ensure coordination and consistency in the comprehensive development of a strategy for risk management within MCCCD. The merger of these committees is called the Maricopa Integrated Risk Assessment (MIRA). On October 27, 2003, Chancellor Gasper assigned responsibility for MIRA to me, Ruth Unks, MCCCD Risk Manager, and asked that I develop and initiate a multi-year implementation plan.

Higher education is no longer insulated from the realities of constant change (if it ever was), and must transform itself to be more responsive to changing business environments and to its stakeholders. Business risks have increased, and it is imperative that MCCCD leaders understand and address those risks. This is done individually as well as across the organization. The MIRA project embraces a wider view of risk—Enterprise Risk Management (ERM), which enables personnel to collaboratively identify, assess and manage future risks and opportunities. This is done individually as well as across the organization. Chancellor Gasper has given the MIRA Committee general outcomes to accomplish. These include:

- Increased overall effectiveness and accountability
- Sound business processes; greater assurance of business continuity
- Clear demonstrated compliance with applicable laws and regulations
- Enhanced employee empowerment and pride
- Reinforcement of the strong Maricopa cultural identity
- Enhanced competitive advantage

A five-year implementation plan was developed to guide the MIRA project. The plan has five sections:

1. Project Planning
2. Evaluate MCCCDC's Environment and Strategy
3. Develop a Comprehensive Risk Framework and Process for Evaluating and Prioritizing Risks
4. Review Risk Financing/Mitigation Options
5. Develop a Risk "Nervous System" for Communication, Reporting, and Monitoring

Dr. Glasper established an ambitious benchmark for the plan—the achievement of the outcomes in the first year of operation, and for each subsequent year after that. He further specified that the plan include the preparation of an annual report for the Chancellor's Executive Council (CEC), comparing the planned and actual outcomes for the year, and submitted to the CEC by August 31 annually.

We encountered several specific challenges as we attempted to implement ERM. Some of the most significant were as follows:

1. Due to our culture, the silo approaches to project activities, and well-protected turfs, it may be difficult to garner the support of MIRA throughout the MCCCDC leadership groups (CEC, deans, and department chairs).
2. Initially, the "new" risk management language will be confusing to employees. A common language and definitions to fit our culture must be developed.
3. There is a perception that there is not a need for Enterprise Risk Management.
4. There is a lack of understanding about what ERM is; buy-in from employee groups may be difficult to achieve.
5. There may not be adequate resources (budget, staff time, etc.) to accomplish the tasks required for full implementation of MIRA.
6. Full integration of traditional risk management and ERM is a new concept; there are not a lot of model programs to follow, specifically for higher education institutions.
7. The traditional risk management program needs to be brought up to date.
8. Employees may not believe that they have adequate time to attend MIRA training, workshops, exercises, etc.
9. MIRA committee members may have difficulty allocating enough time to be fully involved in the MIRA committee initiatives.
10. The process to create and adopt administrative regulations is slow and may delay certain parts of the implementation.

Despite these challenges, the MIRA committee has achieved many accomplishments so far, including:

- Creation and implementation of an ERM implementation plan
- Establishment of the MIRA committee
- Development of a committee charge
- Adoption of a Risk Environment, Culture and Appetite Description
- Creation of Risk Register/Best Practices
- Creation and plotting of risks on a Risk Map
- Development of a mitigation plan to deal with risks
- Development of customized risk assessment tools
- Creation of a website
- Development of a marketing campaign
- Development of risk assessment training courses
- Adoption of an Administrative Regulation
- Publishing of four Annual Reports

The MIRA Committee continues to work towards its goals. Our many accomplishments to date have resulted from the collaborative efforts of many employees who have given their time, wisdom, and experience to make this project successful. By educating employees about risk management and giving them resources to identify and assess risks, employees are now empowered to make well-informed decisions regarding the opportunities and risks of new programs and activities, as well as being accountable for these decisions.

From a personal and professional viewpoint, as chair of the MIRA project, I have gained significant insight into the many risks and opportunities present in MCCCCD's daily operations. I am involved with our strategic planning committee, report regularly to the Audit/Finance Committee, meet annually with the Chancellor's Executive Council, meet with the Faculty Executive Committee, and I am involved with training all 10,000+ MCCCCD employees. I am no longer perceived as the "insurance person," but as the risk advisor, and employees no longer view risk management as a negative process.

MIRA's success depends on the coordinated and cooperative response from employees on every level—individually and collectively. One of the biggest lessons we learned is that we needed to have top-level support, commitment and participation. We were fortunate because our chancellor is the "champion" of our ERM initiative, and he has given the MIRA committee and me his full support. However, the support of certain key employee constituencies has been challenging due to a lack of understanding regarding risk management. By continuing to follow our implementation plan, step-by-step and little by little we will educate our employees so that they will deliver high-quality education to our students in a more efficient and cost-effective manner.

Appendix D—How to Make It Work: ERM at University of California

University of California (by Grace Crickette, Chief Risk Officer)

- Total Student Population: 214,298
- Undergraduate Students: 163,302
- Graduate Students: 45,884.
- Employees: 175,079
- Total Revenues: \$19,991,187,000 (2006)
- Total Organized Research Funds: \$3,035,949,000 (2006)
- Public/Private: Public

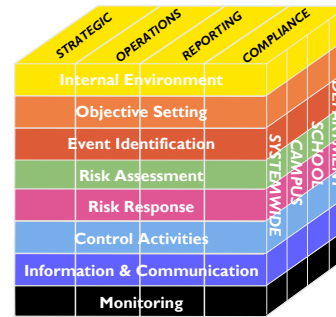
The University of California first opened its doors in 1869. Today, the UC system includes more than 214,000 students and more than 175,000 faculty and staff. UC's ten campuses at Berkeley, Davis, Irvine, Los Angeles, Merced, Riverside, San Diego, San Francisco, Santa Cruz, and Santa Barbara foster world-class educational and research opportunities and generate a wide range of benefits and services that touch the lives of Californians every day. UC's five medical centers support the clinical teaching programs of the University's medical and health sciences schools and handle more than three million patient visits each year. The medical centers provide a full range of health care services in their communities and are sites for the development and testing of new diagnostic and therapeutic techniques. Collectively, these centers make up one of the largest health care systems in California.

The University has been moving towards an enterprise approach to identifying and managing risk, including financial, business, operational and governance risk, since 1996. As a leading institution of higher education and financial practices, the University of California is working to implement the Enterprise Risk Management framework advocated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Our timeline worked this way:

- Regents adopt COSO framework (1996)
- Controller positions established at each campus (late 1990s)
- Several campuses develop ERM initiatives (2004–present)
- Chief Risk Officer (CRO) position established (December 2004)
- ERM Panel formed to develop an ERM strategy (June 2005)

The CRO was hired from the private sector and has experience in using the COSO framework in implementing ERM for private industry.

In the *Statement of Ethical Values* adopted by the Regents in May of 2005, the UC system indicates that “Internal controls are the processes employed to help ensure that the University’s business is carried out in accordance with these Standards, University policies and procedures, applicable laws and regulations and sound business practices. They help to promote efficient operations, accurate financial reporting, protection of assets and responsible fiscal management.... The University has adopted the principles of internal controls published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.” As such, the adoption of the COSO ERM framework was the next logical step in creating an environment that looks beyond just internal controls related to the original COSO framework.



ERM Workgroups at UC

The campuses and medical centers in the UC system operate with a high degree of autonomy, and ERM efforts have been locally driven in large part. Many of the campuses already have ERM groups in existence. At some locations, the groups were created as part of other, ongoing ERM activities; at other locations, existing groups or committees have expanded their charters and range of activities to incorporate their ERM efforts. The longest-standing group, at UC Davis, has existed since 2003 and is a good example of how such campus- and medical center-based groups can effectively address risk across the enterprise. The members of each location’s ERM group come from multiple disciplines; at UC Davis the group is made up of representatives from more than a dozen different departments. This facilitates sharing of cross-disciplinary expertise and gives all members of the group a more complete understanding of the risks faced that might prevent UC Davis from completing its strategic plans. Groups usually include representatives from areas such as Risk Management, Materiel Management, Workers’ Compensation, Environmental Health and Safety (EH&S), Internal Controls, Internal Audit, and the Controller’s office.

Centralized ERM activities at UC are being driven by the Chief Risk Officer. The ERM Panel includes management representatives from Office of the President and the campuses. Panel membership currently includes the EH&S Director (UCOP), the Associate Vice President—Human Resources and Benefits (UCOP), the Vice President—Financial Management (UCOP), the UCOP Emergency Manager and Facilities Administration Coordinator, the Vice Provost for Research (UCOP), the Chief Risk Officer (UCOP), the Director for Systems Development (UCOP), the Associate Vice President—Information Resources and Communication (UCOP), University General Counsel (UCOP), UC Berkeley’s Chief of Police and Director of Public Safety, UC San Diego’s Assistant Vice Chancellor/Controller, the Controller for Agriculture and Natural Resources (UCOP), the University Auditor (UCOP), the Director of Financial Controls and Accountability (UCOP), and the Director for Research (UCOP).

The Office of Risk Services sponsors and coordinates other groups that are also addressing ERM issues. The University of California Risk Management Leadership Council (RMLC) is an organization of Risk Management senior leadership from throughout the UC system. RMLC workgroups have been formed to address risks and issues in the areas of Camps; Driver and Vehicle Safety; Fine Arts; Foundation and Support Groups; Student-Related Risks; Information Technology; Academic Personnel; and Volunteer Clinical Faculty. RMLC members also serve as liaisons to other system-wide workgroups, such as Ergonomics; Emergency Managers; Fleet Managers; Graduate Medical Education Committee; Hazardous Waste Action Group; Research Compliance Advisory Committee; Sports Recreation; Workers' Compensation; and TRIPSS (Field Safety/Travel).

The Office of Risk Services sponsors an annual Risk Summit that brings together UC employees from many various disciplines. Participants include Risk Management, Environment, Health and Safety, Emergency Management, Sports and Recreation, Workers' Compensation, Occupational Health, Disability Management, General Counsel, Human Resources, and others. Risk Summit 2007 was a two-and-a-half day event attended by more than 250 people. Each year attendance at the Risk Summit has increased as it is being expanded to bring in other players with a key role in achieving our goal. The event provided opportunities for education and training, updates on risk management issues, introducing and sharing new ideas, and creating awareness of the universal risks shared throughout the University, as well as providing the opportunity to strategize as a team on ways to reduce those risks.

Environmental Health and Safety sponsors eleven system-wide workgroups: Ergonomics; HWAG (Hazardous Waste and Action Group); Radiation Safety; Bio Safety; Industrial Hygiene/Lab Safety; Fire Marshal; Emergency Management; Environmental Management; Environmental Health; STEW (Safety Training and Education Workgroup); and Field Safety.

ERM Tools

RMIS System

The University retained KPMG International to assist us in reviewing existing programs and data to identify which components of the ERM framework are in place, which components need to be expanded or improved, and which components do not yet exist at UC and will need to be implemented. During a series of visits to each of the ten campuses and five medical centers within the UC System and the Division of Agriculture and Natural Resources (ANR), we met with more than 425 key stakeholders in areas such as employment practices, infrastructure and construction, student life, strategic sourcing, budget, safety and emergency preparedness, research, internal controls, IT risk, and more. In order to encourage participants to freely contribute their knowledge and concerns during the meetings, we chose not to use an anonymous voting system such as OptionFinder, instead using time-honored technology like flip pads and markers to record ideas contributed during the meetings. Using information from the stakeholder interviews, a preliminary list of more than 550 possible leading indicators (LIs) were identified, of which approximately 430 are unique—that is, not duplicated at any of the other campuses or medical centers. Although not all of these LIs can be tracked at this time due to limitations on data collection and gathering, the next stage of the project is to determine how those LIs can be effectively represented in a dashboard report housed in a Risk Management Information System (RMIS), which is being developed with the assistance of UCOP Information Resources and Communications. A draft report is being prepared which will include analysis of which LIs can or cannot be created using already-existing information. The RMIS will deliver dashboard technology for reporting ERM activity, a platform for monitoring risks and controls at the campus or medical center level, and the ability to have an ongoing risk assessment platform.

ERM Toolkit

We are working to make the ERM section of our webpage a central resource for ERM knowledge system-wide. It currently includes a library of documents and links to information, both internal and external, and an ERM “toolkit” that includes sample ERM group charters, work plans, strategic goal plans, surveys, and strategic risk assessments.

Challenges and success stories

Challenges to implementing ERM include UC’s size and decentralized nature, and the high degree of autonomy with which each campus and medical center operates. Local administration sees more clearly the ways in which their location differs from the others, while the more centralized perspective that OPRS has allows us to see the commonalities among the risks and challenges facing the locations. Rather than attempt to impose a top-down ERM program by Presidential or Regental decree, we have chosen a bottom-up approach. By making better use of data already being collected and risk management activities already in existence without imposing new requirements, we will be able to demonstrate the benefits of ERM to the locations and gain campus and medical center support for future stages of implementing ERM throughout UC.

We are working to develop a data warehouse that can manage information already being collected by various groups, existing programs, and initiatives throughout the system. Once consolidated in a single Risk Management Information System, the data can then be used with the COSO framework

to analyze processes, risks, and controls system-wide. Local ERM panels will have full use of this tool to aid in their risk assessments, monitoring of risk and controls, and producing business intelligence dashboards and reports. The local panels will be the owners of the RMIS system; the Office of Risk Services is coordinating and facilitating, not directing.

- In addition to the locations that already had ERM groups, in the last year three locations have developed new ERM groups: UC Riverside, UC Merced, and the UC San Diego Medical Center. And although UC Berkeley's group has not been officially formed yet, they are already doing ERM work. Here are some things that are happening at specific locations:
- In addition to developing their charter, UC Riverside's ERM group has developed a list of ERM objectives based on UCR's strategic goals. UCR's Controller will be conducting an ERM survey to assess departments' alignment with the ERM objectives. Committee members represent a broad array of administrative departments, plus a smattering of others including Office of Research, Health Center, Audit, etc.
- UC Merced's new ERM group is charged with advising the Vice Chancellor for Administration by collaborating to identify and manage the full range of risks UCM faces. Panel membership includes the Assistant Vice Chancellor of Business and Financial Services, the Director of Campus Recreation, the Controller, the EH&S Director, the Chief of Police, the Director of Purchasing, the Assistant Vice Chancellor for Human Resources, the Associate Vice Chancellor for Research, the Director of Institutional Planning and Analysis, and a designee from the Academic Senate. The Chief Risk Officer is serving on the Panel in an advisory capacity as they come up to speed.
- The UC San Diego Medical Center has determined that it will hold special sessions of the Senior Management Team (which has physician representation), which will be designated as the ERM Advisory Committee. Their charter, currently under development, includes a charge to disseminate through the clinical enterprise an understanding of the "upside" of risk—risk as opportunity, not merely hazard. Committee membership includes the UCSD-MC CEO, COO, CFO, Physician-in-Chief, CMO, CNO, the Corporate Compliance Officer, the Director of Human Resources, the Chief Risk and Safety Officer, and the Medical Group COO.
- UC Berkeley's ERM Initiative Steering Committee has not yet been formalized, but work is already underway. Work to date has focused on identifying risks, risk ownership, and data; future activities include development of comprehensive risk management policy, prioritization of risks, and increased communication with the campus community.

- UC Davis's ERM Group has been active since 2003 and has conducted enterprise risk assessments focused on risks that might prevent UCD from completing its strategic plans. The workgroup is made up of representatives from more than a dozen different departments.
- UC Irvine's ERM Council includes members from Materiel and Risk Management, Workers' Compensation, EH&S, Internal Controls, Internal Audit, and the Controller's office, and is reviewing membership to determine which other groups should be included (such as Academic Personnel). The Council is evaluating ERM techniques and working on ways to implement ERM into the UCI culture.
- The UCLA Controls Work Group was established by the Chancellor to provide oversight to the strengthening and maintenance of UCLA's systems of internal control and accountability. It meets on a regular basis to monitor campus control systems and help ensure the deployment of reasonable and understandable policies and procedures across the campus. The group has expanded its charter and range of activities to address ERM issues as well.
- UCSB's Control Advisory Committee's focus to date has been financial risk, but the group plans to expand into ERM activities.

ERM Advice and Lessons Learned

Rather than trying to create and impose one top-down program, our focus is on supporting the development and strengthening of the local ERM Panels. Seven campuses/medical centers have already formed ERM groups, without the "aid" of any particular policy. They have done so because they see a value in forming these groups and being proactive in managing their risk. Many of the locations that do not have official "ERM groups" have other groups or committees that are expanding their charters to include ERM, and groups are being created at the remaining locations. The ERM Panel, OPRS, and other internal and external experts will provide regular and ongoing support to the ERM groups in the way of consultation, presentations, and tools, but will not be the driving force behind ERM. ERM has become a "grass-roots" movement at UC, and "taking it too corporate" would be counter-productive.

Suggested Tools, References, and Resources for More Information

The following references materials are excellent tools for implementing Enterprise Risk Management on campus. They have been selected for their clarity in describing the ERM process and for the examples of specific tools they provide to aid in implementation. (Definitions of common terms used with Enterprise Risk Management can be found in the *Glossary of Terms* below.)

For basic references:

- *Enterprise Risk Management for Dummies*, distributed by the Risk and Insurance Management Society, Inc (RIMS) (Wiley Publishing, 2007).
- *Excellence in Risk Management II: A Qualitative Survey of Risk Management Programs*, co-published by RIMS and Marsh, Inc., 2005.

To better understand the origins of ERM:

- *Enterprise Risk Management—Integrated Framework; Application Techniques*, by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004.

For references on implementing ERM specific to colleges and universities:

- *Achieving Goals, Protecting Reputation: Enterprise Risk Management for Educational Institutions*, by PricewaterhouseCoopers.
- *Developing a Strategy to Manage Enterprisewide Risk in Higher Education*, by the National Association of College and University Business Officers (NACUBO), 2001.

Maricopa County Community College District has implemented ERM on their campuses. For references specific to their implementation plan and an example of an annual report, refer to the link at <http://www.maricopa.edu/mira/communications.php> and look for these documents:

- *Implementation Plan for Maricopa Integrated Risk Assessment Project*, Maricopa County Community College District, by Ruth A. Unks, November 25, 2003.
- *Maricopa Integrated Assessment Annual Report*.

Where to find information and tools in the references cited above

	ERM for Dummies	Excellence in Risk Management	COSO	PwC	NACUBO	MCCCD Implementation Plan/Annual Report
COSO Framework			●			●
Management Support		●				
Campus Planning Process						●
Risk Assessment	●		●			●
Risk Maps	●		●	●		●
Case Studies	●		●		●	
Creating ERM Culture		●			●	●
Risk Communications			●			●
Monitoring ERM			●			●
Role of Internal Audit			●	●	●	
Best Practices	●		●	●		●

The Risk and Insurance Management Society, Inc. (RIMS) has developed the *ERM Center of Excellence*, which is a comprehensive source for tools, papers, studies and news related to ERM. General information is available on the main website; more specific information is available at: <http://www.rims.org/Content/NavigationMenu/ERM/ERM1/ERM.htm>

RIMS has also developed the *Risk Maturity Model*, which is a tool to help you evaluate your risk management program and take it to the next level. The RIMS Risk Maturity Model is an online resource that provides guidelines and best practices for developing and maintaining risk management programs and can be found at:

<http://www.rims.org/Content/NavigationMenu/ERM/ERM1/ERM.htm>

Basic Frameworks for Risk Management is a report prepared by John Shortreed, John Hicks, and Lorraine Craig for the Network of Environmental Risk Assessment and Management (NERAM) provides an overview of frameworks for ERM. The report describes how a “standard” framework can be adapted for use by various organizations. The report can be accessed at: http://www.rims.org/%5CResource_Library%5Cdocs%5Cefdqelgd.pdf

In *The Role of Internal Auditing in Enterprise-wide Risk Management*, published by the Institute of Internal Auditors, the core role of internal audit is discussed with regard to ERM. This article can be found at: http://www.rims.org/%5CResource_Library%5Cdocs%5Cojlkjlr.pdf.

AS/NZS 4360:2004, The Australia-New Zealand risk management “standard,” is considered by some to be the gold standard for all other standards and has, in fact, been used as the benchmark by ISO in the development of their standard. The AS/ZN development committee describes it as a “generic framework for establishing the context, identifying, evaluating, treating, monitoring and communicating risk.” Any organization can adapt this framework to individual circumstances. This standard can be obtained at: <http://www.riskmanagement.com.au/>.

HB 436, *Risk Management Guidelines-Companion to AS/NZS 4360:2004* contains specific guidance regarding the implementation of the AS/NZS 4360:2004 Standard. The two documents are intended to be used together. This handbook is a clear, step by step, “how-to” guide and can be obtained at: <http://www.riskmanagement.com.au/>.

“Enterprise Risk Management: A Fundamental Practice for Higher Education,” an article in the 2003–2004 *URMIA Journal* written by Jane Dickerson, Peter Fallon and Leta Finch, discusses the benefits of implementing an ERM program, how to get started, and how to identify and analyze risk. The article also showcases the ERM programs at UNC at Chapel Hill, the University of California at Davis and the University of Notre Dame. Available to URMIA members at: <http://www.urmia.org/library/docs/2003urmia.journalfinal.pdf>.

“Developing a Strategy to Manage Enterprisewide Risk Management in Higher Education” is a paper presented by NACUBO, in conjunction with PricewaterhouseCoopers. This paper discusses the practical implementation of effective enterprisewide risk management in higher education, with focus on the definition of risk/risk drivers, implementation of a risk management program, and how to proactively

engage the campus community in dialogue around ERM. <http://www.pwc.com/extweb/pwcpublications.nsf/docid/BA1AB197F0775715852572FF007F50D2>

“Achieving Goals, Protecting Reputation: Enterprise Risk Management for Education Institutions” is a 2006 paper issued by PricewaterhouseCoopers which discusses applying the COSO model. This paper discusses the steps institutions can take to implement ERM strategies.

<http://www.pwc.com/Extweb/pwcpublications.nsf/docid/A5E9AF853DD1665F8525721F006F7048>

The paper entitled “Enterprise Risk Management—Integrated Framework,” issued by COSO in September 2004, is a must read for every organization embarking on the implementation of an ERM program. The report is in two volumes. The *Executive Summary*, a high level overview of the framework is available at <http://www.coso.org>.

Enterprise Risk Management for Dummies by Beaumont Vance and Joanna Makomaski (Wiley Publishing) is described as “a valuable start up guide for ERM first timers.” Utilizing the traditional RM five-step approach, this book is a practical start-up guide and is available at www.rims.org.

“Excellence in Risk Management II: A Qualitative Survey of Enterprise Risk Management Programs” is a joint report issued in September 2005 by RIMS and Marsh. This report provides feedback from five large North American companies in the process of implementing ERM programs. The document discusses the importance of having senior management support for ERM, of having a clear framework/process, and of building ERM into an organization’s corporate culture. It is available at <http://www.rims.org>.

Issued in 2006, also by RIMS and Marsh is a report entitled “The Changing Face of Risk Management.” This report summarizes a quantitative survey of RIMS members regarding the current state of risk management, how risk managers are responding to the new world of risk and the future direction of risk management. Of the companies responding to the survey, 4% have fully implemented ERM, 22% partially implemented and 47% are considering or planning implementation. Available at <http://www.rims.org>.

A Guide to Enterprise Risk Management: Frequently Asked Questions is a publication issued in January 2006 by Protiviti and meant to answer frequently-asked questions relating to initiating, developing and implementing an ERM program and the COSO framework. This extensive publication is supplemented by the bulletin entitled “Enterprise Risk Management: Practical Implementation Advice,” an executive-level ERM overview. Download from <http://www.protiviti.com>.

Enterprise-Wide Risk Management for Corporates by James DeLoach and Nick Temple (Pearson Education Limited, 2000) guides you through the key stages of designing and implementing an integrated enterprise-wide risk management program.

“Enterprise Risk Management: Practical Implementation Ideas” is a paper written by James DeLoach, Managing Director of Protiviti, and presents general information regarding the principles of ERM and a stepwise approach for implementing an ERM in an organization. Download from:

<http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/InternalAuditEnterpriseRiskManagementPracticalImplementationIdeas!OpenDocument>.

Glossary of Common Terms Associated with Enterprise Risk Management

Note: the following definitions have been borrowed from Maricopa County Community College District's ERM definitions, except when another source is noted, and have been edited to be more universal.

Audit Cycles (definition from the University of Minnesota)

Audit coverage of departments on regular cycles based on its risk assessments. For example:

- High-risk departments are scheduled to receive audit coverage every three years
- Above-average risk departments are scheduled to receive audit coverage every four years
- Moderate risk departments are scheduled to receive audit coverage every six years
- Low-risk departments are scheduled to receive audit coverage every eight years.

Audit Department Risk Assessment (definition from the University of Minnesota)

An Internal Auditor might employ a formalized risk assessment methodology in selecting departments for inclusion in an annual audit plan. The assessment measures a department's overall risk relative to other college or university departments. The risk factors considered in a department's assessment may include:

- Level of sponsored and non-sponsored revenues and expenditures
- Impact of unit/process on other institutional activities
- Significant system development or process change
- Regulatory compliance issues
- Pending or potential litigation issues
- Organizational change/turnover
- Known or perceived control concerns
- Audit history

Based on the outcome of the assessment, individual departments are categorized into one of four risk levels: *high*, *above average*, *moderate*, or *low risk*. A rating of "*high risk*" does not necessarily mean a department is perceived to have control problems, but rather is a reflection of the criticality or impact of the department to the institution's mission.

Chief Risk Officer (CRO)

A senior manager with day-to-day oversight of enterprise risk management.

COSO (definitions from COSO)

The Committee of Sponsoring Organizations (COSO) Treadway Commission is a voluntary private sector organization. It is dedicated to helping improve the quality of financial reporting through business ethics, effective external controls, and corporate governance.

According to COSO, the three primary objectives of an internal control system are to "ensure efficient and effective operations, provide accurate financial reporting, and comply with laws and regulations."

It is sponsored by the five major financial professional associations in the United States: the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives Institute, the Institute of Internal Auditors, and the Institute of Management Accountants.

COSO provides a model to achieve its recommended internal control process that includes:

- Evaluating the effectiveness of existing internal controls
- Identifying high risk/reward areas, including disclosing risks that could adversely effect the institution
- Determining the appropriate level of controls to better manage the risks
- Comparing the current situation with target goals
- Implementing procedures to minimize risks

COSO (definition continued)

- Ensuring that reporting and documentation can pass scrutiny by third party evaluators
- Communicating improvements to employees and training employees to report deficiencies to management
- Establish and implement a formalized monitoring process and establish a mechanism to ensure continuous improvement.

Cost-of-Risk

The financial impact of an organization from undertaking activities with an uncertain outcome and includes such factors as the cost of managing those risks, financially transferring the liabilities, and sustaining any uninsured losses.

Common Cost-of-Risk Measurements or Risk Ratings are:

- Frequency
- Severity
- Cost to mitigate
- Total cost-of-risk
- Degree of uncertainty
- Benefits to the institution
- Financial value
- Institutional enhancement

Enterprise Risk Management (ERM)

An integrated approach to assessing and managing all risks that threaten a college or university's ability to achieve its strategic objectives. The purpose of ERM is to understand, prioritize, and develop action plans to maximize benefits and mitigate risks of greatest concern to the institution. The ERM framework enables management to work collaboratively to identify, assess, and manage existing and future risks that are integrated across campus in various ways, also known as *holistic*, *strategic*, or *integrated* risk management. ERM:

- is central to an institution's strategic planning and management

- is focused on identifying and treating risks of all types
- adds maximum sustainable value to all activities
- increases probability of success and minimizes probability of failure
- is continuous; integrated with strategic planning and plan implementation
- is integrated with organizational culture and led by senior management
- assigns responsibility throughout the organization in each position description

Financial Benchmarks

- Primary Reserve Ratio: Illustrates how long an institution can survive if it were to totally shut down.
- Net Operating Revenue Ratio: Determines whether the institution operates in a surplus or deficit.
- Return on net assets ratio: rate of effective deployment of resources; net income divided by net assets
- Viability ratio: Ability to meet debt obligations with expendable assets.

All of these calculations take into consideration the historical costs-of-risk. What they don't do is expose any gaps in coverage or other protections.

Impact

Result or effect of an event. The impact of an event can be positive or negative relative to the entity's strategic objectives, and there can be a range of possible impacts associated with any single event.

Inherent Risk

The risk to the college or university in the absence of any actions management might take to otherwise alter the likelihood the risk could result in an event with a negative impact.

Internal Environment

Encompasses the culture of a college or university and sets the basis for how risks are viewed and managed, including risk management philosophy, risk appetite, integrity and ethical values, and the overall environment in which the organization operates.

Likelihood

The possibility that a given event will occur.

Loss Control

The technique of minimizing the severity of loss or the impact of any negative event once it occurs.

Metrics

The means in which to measure the effectiveness and/or success of risk mitigation strategies.

Opportunity

The possibility that an event will occur that will have a positive impact on the institution and the achievement of its strategic objectives.

Performance Assessment (definition from Protiviti's *Guide to Enterprise Risk Management*)

The retrospective activity applied to evaluate the performance of a unit, a process or a function against a pre-determined target or standard over a state period of time.

Residual Risk

The risk that remains after the institution has employed risk strategies/mitigation.

Risk

- a) The combination of the probability of an event and its consequences. Risk is inherent in all types of undertaking and may carry the potential for benefit or be a threat to success.
- b) The opportunities, uncertainties, threats, and barriers to which a college or university must respond in order to achieve its objectives.

Risk Acceptance

Occurs when no action is taken to affect a risk's likelihood from developing into an event resulting in a negative impact on the institution.

Risk Analysis

Identifying and describing risks and estimating the impact of each on the institution, and developing corresponding risk profile.

Risk Appetite (definition from COSO)

An organization's tolerance for risk. The broad amount of risk a college or university is willing to accept in pursuit of its mission or vision. The measurement of risk appetite may be evaluated qualitatively or quantitatively.

Risk Assessment

Determining the impact of an identified risk on the institution. Risks are assessed on an inherent and residual basis.

Risk Assessment Activities

- *Risk identification*—the qualitative determination of significant risks that can potentially impact the institution's achievement of its financial and/or strategic objectives. This is often done through structured interviews of key personnel by internal or external experts.
- *Risk prioritization*—the ranking of risks on scale, such as frequency and/or severity (see **Risk Mapping**).

Risk Assessment Tools

Instruments designed to assist colleges and universities in assessing and evaluating risks in order to make more informed decisions.

Risk Avoidance

Avoiding the activities giving rise to risk.

Risk Categories

- . *External*: Exposure to uncertainty affecting the community(ies) served by the college or university.
- . *Financial*: Exposure to uncertainty regarding the management and control of the finances of the institution.
- . *Hazard*: Exposure to loss arising from damage to property or from tortious acts; typically includes the perils covered by insurance.
- . *Human Resources*: Exposure to uncertainty related to compliance with personnel policies and procedures, employee morale, and organizational culture.
- . *Legal/Regulatory Compliance*: Exposure to uncertainty related to laws, statutes, and administrative regulations that govern how colleges and universities operate.
- . *Operational*: Exposure to uncertainty related to day-to-day business activities.
- . *Reputational*: Exposure to uncertainty related to brand, perceived value, organizational status, and public perception and trust.
- . *Strategic*: Exposure to uncertainty related to long-term policy directions of the institution—the “big picture” risks.

Risk Control

The technique of minimizing the frequency or severity of potential losses through training, safety procedures, and engineering and security measures.

Risk Evaluation

Comparing the results of estimating risks to the significance of the risks to decide whether to accept and manage them, transfer them by means such as insurance, a combination of the two, or eliminate the risks all together.

Risk Financing

The mechanisms for funding risk mitigation strategies and/or funding the financial consequences of risk; i. e., insurance or the financial consequences of uninsured risks.

Risk Identification

The qualitative and, whenever possible, the quantitative determination of risks that are material; i. e., that potentially can impact the achievement of the institution’s strategic objectives.

Risk Mapping

The visual representation of risks which have been identified through a risk assessment exercise in a way that easily allows priority ranking of them. This representation often takes the form of a two-dimensional grid with *probability* on one axis and *impact* on the other axis. The risks that fall in the high probability/high impact quadrant are given priority risk management attention.

Risk Mitigation

Actions which reduce a risk or its consequences (see **Risk Strategies**).

Risk Portfolio

A list of risks identified and evaluated by a college or university (also called *Risk Register*) that represent a portfolio of risks at a certain time.

Risk Prioritization

The ranking of material risks on an appropriate scale, such as frequency and/or severity (see also **Risk Mapping**).

Risk Profile

The use of a tool or system to rate and/or prioritize a series of risks.

Risk Reduction

Action taken to reduce risk likelihood or impact, or both of frequency or severity of potential losses. May include risk transfer, engineering, fire protection, and/or safety inspections.

Risk Response

Management selection of risk avoidance, acceptance, reduction, or sharing risk, and developing a set of actions to align risks with the institution's risk appetite and tolerances.

Risk Reporting

Distribution of information on risks to internal and/or external stakeholders.

Risk Sharing

Reducing risk likelihood or impact by transferring some or otherwise sharing a portion of the risk.

Risk Strategies

Possible responses to risk situations such as avoidance, acceptance, sharing, and reduction.

Risk Tolerance

The acceptable level of risk relative to the achievement of an objective.

Risk Treatment

The process of selecting and implementing measures to modify the risk.

Sarbanes-Oxley Act

The *Sarbanes-Oxley Act of 2002*, commonly referred to as "SOX" or "SarBox," is an amendment to the Federal Securities Exchange Act of 1934. It is intended to prevent auditors from providing specific non-audit services, including actuarial services, to their SEC-regulated audit clients. There are five major components of the amendment that are of specific interest for higher education. They include sections on 1) transparency of financial reports, 2) corporate disclosure, 3) board independence, 4) accountability, and 5) development of ethical operating standards. Although the Act includes requirements that apply to publicly held companies only, some higher education trustees believe that some or all of these components are essential to good practices for colleges and universities.

Silo

Divisions, departments, or other groups and individuals on campus that tend to act in isolation from one another.

Traditional Risk Management

Original form of risk management, focusing primarily on insurable *hazard* risks.

Bibliography

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management—Integrated Framework*. New York: 2004.

International Organization for Standardization (ISO). *Risk Management—Guidelines on Principles and Implementation of Risk Management*. WG on Risk Management Secretariat: Working Draft 3 of AWI 25700, 2006.

Joint Standards Australia/ Standards New Zealand Committee. *Risk Management Guidelines*. Standards Australia/Standards New Zealand, 2004.

Shenkir, William G. and Paul L. Walker. *Implementing Enterprise Risk Management*. Institute of Management Accounting, 2006.

University of Regina. *Enterprise Risk Management Framework*. November 2006.



**University Risk Management
and Insurance Association**

URMIA National Office
P.O. Box 1027
Bloomington, IN 47402
www.urmia.org

Appendix B: “Credit Rating Analysis of Enterprise Risk Management at Nonfinancial Companies: Are You Ready?”

Credit Rating Analysis of Enterprise Risk Management at Nonfinancial Companies: Are You Ready?

Enterprise risk management (ERM) initiatives appear to be gaining strong support from a new source: credit rating analysts. In November 2007, Standard & Poor's (S&P) issued its *Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Nonfinancial Companies* (RFC), reflecting the rating service's intention to assign scores of ERM quality to all companies it reviews and incorporate an ERM segment into its ratings reports.

Considering ERM in the ratings process is not new. Like Moody's Investors Service, S&P always has probed the risk management processes of financial institutions and insurers. In recent years, both S&P and Moody's have extended their formal evaluation of these processes to those entities using an ERM-like framework. Moody's reports that it integrates risk management capabilities into all of its credit ratings. Meanwhile, S&P has begun extending the consideration of ERM to power generation companies. Finally, other rating services disclose that they consider various aspects of ERM in their ratings of insurers and financial institutions.

Now S&P is seeking comment on a move that would affect thousands of public and private companies in dozens of industries by expanding the evaluation of ERM capabilities into nonfinancial sectors. This move creates a possibility of reduced debt ratings if the firm's analysts conclude there are gaps in the risk management capabilities of the nonfinancial companies they cover. This issue of *The Bulletin* explores how consideration of ERM quality can impact the ratings process and what nonfinancial companies can do to prepare for this added dimension to the process.

S&P's point of view

In the aftermath of Katrina, the recent massive product recalls, the discovery of another record-setting loss from a rogue trader at a French bank and, of course, the sub-prime mess, the ratings process has never been under closer scrutiny. Companies can expect the rating agencies to play this one carefully and tough. The principal objective in evaluating ERM is to drive companies to implement

practices that will limit the frequency and severity of losses that could potentially affect ratings.

The S&P RFC proposes to introduce ERM analysis into the corporate credit ratings for nonfinancial companies as a forward-looking, structured framework to evaluate management's overall capabilities, faithfulness in executing a sound strategy and adaptability to a changing operating environment. S&P points out that "the quality of management judgment is not as easily benchmarked by quantitative metrics in the way that ratios and models of cash flow adequacy, liquidity, earnings capacity, and leverage [can]." S&P's plan to solicit feedback from the market is intended to help it evaluate whether this change would help it provide more accurate ratings.

S&P proposes to score companies to benchmark its opinions on ERM quality. The firm's purpose is to use the deterioration or improvement over time in a company's ERM quality to gauge rating and outlook changes before the consequences of extreme adverse events manifest themselves in published financial reports. In essence, S&P brings a creditor's bias to evaluating a company's ERM capabilities in a forward-looking manner, as evidenced by its comment that "a firm's future ability to meet financial obligations in full and on time is more likely to be enhanced by strong ERM or diminished by weak or non-existent ERM." The message is that rating agencies appear to be tying their historical sensitivity to significant and volatile unexpected losses to the rated entity's ability to understand such volatility and prudently manage these risks through the application of ERM.

Recognizing that ERM is not a one-size-fits-all cookbook for all industries and that each company must tailor the ERM process to its specific circumstances, S&P's evaluation framework is based on the following analytic components: risk management culture and governance, risk controls, emerging risk preparation and strategic risk management. These four components are discussed next.

Risk management culture and governance

S&P seeks evidence that risk and risk management are important factors in day-to-day decision-making. The analyst will evaluate the organizational structure, as well as roles and responsibilities, competence and accountabilities of the individuals who execute risk management. For example, he or she might inquire as to whether management has articulated the firm's tolerance for risk, delineated the staff responsible for risk management, defined their reporting relationships, communicated the company's measures of their success, integrated risk management into performance management and budgeting, and clarified how metrics around risk management affect compensation.

Culture and governance are important because they are indicators as to the extent of integration and influence of risk management on corporate decision-making. A strong ERM process is one that makes risk transparent in corporate dialogue and communications up, down and across the organization by establishing risk tolerances and making them explicit in the day-to-day execution of the business model. Compliance with regulatory standards is not enough. In fact, S&P states:

An excessive compliance culture may belie a weak risk management culture. This is because a compliance approach to risk management usually means that the firm has neglected self-assessment and prioritization of risks and risk management activities, leaving those roles to the regulator.

Risk controls

The RFC states that “firms achieve risk control through identifying, measuring, and monitoring risks, setting and enforcing risk limits, and managing risks to meet those limits through risk avoidance, risk transfer, risk offset, or other risk management processes.” S&P expects to see programs in place that can be expected to effectively deliver the risk controls necessary to manage exposures and losses within established limits, as well as drive “consistent execution ... so that future implementation will be a given.” S&P's PIM approach (policies, infrastructure and methodology) will focus the analyst's inquiry:

- **Policies** include business strategy, risk tolerances, risk authorities and disclosure requirements to be addressed through internal and external reporting.
- **Infrastructure** includes personnel, back-office operations, data and technology.
- **Methodology** includes risk metrics, stress testing, validation activities and performance measurement.

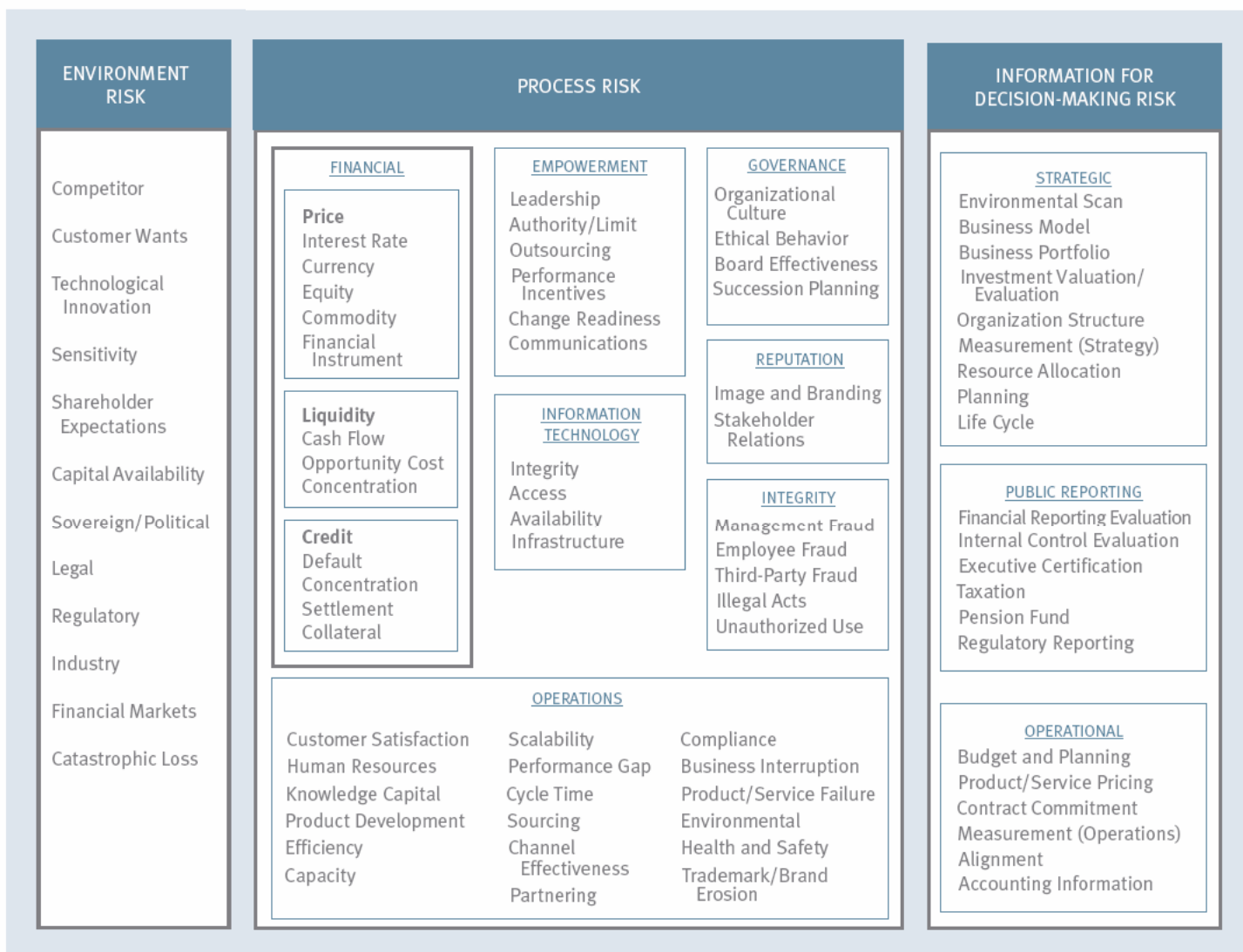
S&P points out that the relative importance of each of these areas to the rating service's overall conclusion regarding risk control quality will depend on the complexity, size and risk tol-

erance of each company. The RFC indicates that the number of risks addressed and the nature of the risk control processes in place will vary by sector and company. Accordingly, S&P plans to develop separate risk control criteria for each sector, and submit those criteria to public exposure and comment before implementation.

Evidential matter is also important. It is unlikely the analyst will merely accept management's oral assertions as to the existence of ERM capabilities without examining some supporting evidence. For example, evidential matter might include, among other things, board minutes, management meeting agendas, a risk committee charter, risk-based policies, the organizational structure, a common risk language, recent risk assessment results, demonstration of selected measurement tools, existence of a risk-adjusted capital framework, and evidence of risks considered in the strategy-setting and business-planning processes. The analyst is likely to want to understand how the company identifies and controls each major risk, including the company's limits for each major risk and how those limits are enforced. If the company experienced a recent loss event, the analyst will seek to understand how the company managed the losses and whether appropriate improvements were made to risk management processes as a result of the loss experience. Reporting to senior management and the board of directors is also likely to be a point of focus. An overview presentation summarizing management's operating philosophy around ERM and how it impacts the business would be useful to set a context for the analyst.

In the RFC, S&P discloses its initial point of view of the key risks facing different sectors. For example, for oil and gas, S&P states the key risks include commodity prices, environmental concerns, natural disasters and weather, a pandemic, expropriation, and regulatory and legislative. For consumer products, the risks include failure to innovate, mergers and acquisitions (M&A) and restructuring, and reputation. For capital goods, engineering and construction, the risks include commodity prices, labor skills shortage, project management, strategic execution, liquidity, M&A and restructuring, and supply chain. There also are other nonfinancial industries for which S&P provides key risks, including airlines, automotive, chemicals, electric utilities, integrated gas, health products, health services, hotel and gaming, media and entertainment, natural resources, retail, technology and telecommunications.

In offering its point of view around key risks, S&P essentially asserts that these risks are the minimum the rating service expects an organization within a given sector to be assessing, prioritizing and managing. Therefore, a company's existing risk model needs to include these risks. For companies without a risk model, the S&P list of risks is a good starting point for customizing one. S&P allows management to consider other risks, which in effect leads to a customized risk model by company. To illustrate the potential risks to consider, we provide an example risk model on the next page.



The above risk model depicts three groupings of risk – environment, process and information for decision-making. These risk groupings provide a broad foundation on which more specific categories of risk can be identified. The risk categories within these three groupings can be customized by industry. The point is that companies need a common risk language with which to begin an enterprise risk assessment. Therefore, they should start with the key risks provided by S&P and add additional risks germane to the successful execution of the organization’s business strategy using examples in the above model. The resulting risk language would provide an excellent context for the application of S&P’s PIM approach.

For more information regarding the above risk model, we have provided a supplement to this issue of *The Bulletin* (see “The Protiviti Risk ModelSM – An Illustrative Risk Language” at www.protiviti.com).

Emerging risk preparation

Risk management is not static; risk profiles constantly change. Recognizing this, S&P defines emerging risks as “those that are

completely new or extremely rare adverse events, and therefore cannot be managed via a control process.” The rating service expects companies to deploy appropriate activities to anticipate adverse events and plan responses to them. These activities include “environmental scanning, trend analysis, stress testing, contingency planning, problem post-mortem, and risk transfer.” Depending on the nature of the business, the analyst will look (a) for evidence that a company is planning for extreme adverse events, as well as (b) for the results of such planning, both during and after the occurrence of such events. The analyst might also inquire concerning the company’s stress testing practices and its contingency plans for extreme disasters. According to S&P, “results will include immediate information on the exposure of the firm to loss from the actual event, a prompt and sure response, the ability to moderate losses, and the ability to establish clear modifications for future procedures.”

Strategic risk management

This component involves integration of risk, risk management and return for risk into the strategy-setting process. The analyst will focus on “understanding the firm’s risk profile, and obtaining

management's explanation of recent changes in the risk profile, as well as expected future modifications." S&P states that the risk profile can be expressed in terms of earnings loss, impact on enterprise value, or through other financial metrics for various risks or for each operating unit. For example, the analyst might inquire as to whether the company uses risk/reward analysis when considering resource allocation decisions in strategic planning, making pricing decisions and measuring performance.

Strategic processes affected by risk and risk management capabilities include capital budgeting, business planning, performance measurement, product management, acquisitions and divestitures, new venture risk/reward standards and incentive compensation, among others. S&P's message in the RFC is that the degree to which risk is a vital factor in managing these and other processes, and the degree to which the management of risk is a priority within these processes, are prime indicators of the quality of strategic risk management.

What to expect next

The S&P RFC comment period expires March 1, 2008. Thereafter, S&P stated it would decide whether to include ERM analysis in the ratings process. Through the RFC process, S&P is obtaining feedback around whether (a) an ERM review would provide significant additional insight into a company's credit quality, (b) an independent opinion about a firm's ERM capabilities enhances the value of the ratings analysis to investors, and (c) the proposed ERM framework (i.e., the four components) adequately captures a company's risks and capabilities to manage them. In addition, the rating service is looking for suggestions for the ERM evaluation process.

While S&P is gauging the readiness of nonfinancial companies, we expect the incorporation of ERM quality into the ratings process to happen. The challenge in implementing this approach is recognizing that nonfinancial companies have different business risks and processes than financial institutions and insurers. Accordingly, different scoring definitions are necessary.

If S&P decides to integrate ERM into its credit ratings, the analyst who covers a company also probably would be in charge of assessing its risk management. Since the ERM assessment will be an integral component of determining the overall business profile, it would result in integrating risk management as one of several other criteria to rate the credit of companies. Companies can expect that analysts would gather internal risk reports and other materials during the evaluation process and discuss with management the company's ERM philosophy and approach. S&P has said that its rating committees would evaluate the findings of its analysts and reach a conclusion about the quality of the ERM process and the importance of ERM to the rating of each firm evaluated.

Reading between the lines of the RFC, we can expect more explicit criteria by sector following S&P's decision to go forward sometime in 2008. The good news is that analysts probably will

refrain from assigning ERM quality scores to individual companies until a sufficient number of companies have been reviewed to allow for comparability across the applicable sector. Therefore, we can expect S&P to benchmark companies within each sector for a period of time before "going live" with an ERM quality score. S&P has said the actual implementation of the ERM quality score could take place in "as little as a few months" and may not occur for "at least one year." This period gives companies time to improve their processes, *if they act soon to prepare*. "Quick fix" solutions won't work and are not sustainable.

What's particularly important for companies to realize is that their ERM process will be regarded as "weak" if: risk management is ad hoc and reactive; risk controls are missing or are limited in effectiveness in managing, one or more critical risks; losses in specific areas are widespread; and risk and risk management are not integrated effectively with corporate decision-making. If S&P regards ERM as an essential aspect of evaluating management quality and the business profile, a "weak" assessment could have an adverse effect on the company's credit rating, particularly if S&P concludes the company has a high level of potential risk exposure.

Some companies are prepared, others are not

The 2007 Protiviti U.S. Risk Barometer study (available at www.protiviti.com), which surveyed 150 senior-level executives from America's largest companies, reports risk profiles are changing as America's largest companies take more risks. It also reports that risk levels, as well as appetite for risk, have changed significantly over the past two years. This is important from a rating service perspective, because increased vulnerability is a key indicator of the importance of ERM quality.

The Risk Barometer reports that just over half (53 percent) of organizations believe they are "very effective" at identifying and managing all potentially significant risks. Using the survey data, we found that "very effective" companies are more likely than the other participating companies to:

- Deploy an enterprisewide risk management policy and a formal enterprisewide risk assessment process
- Implement a risk monitoring and reporting process
- Formally integrate the risk assessment process and the risk responses for key risks with business planning and strategy-setting activities
- Quantify risk to a greater extent
- Maintain an appropriate balance between the activities for controlling the business and the activities driving entrepreneurial and opportunity-seeking behavior

The message is that companies with more sophisticated risk management infrastructure are less ad hoc and more anticipatory in improving their capabilities continuously, and therefore will be more effective in avoiding surprises and keeping pace with changing risk profiles. Rating services are looking for precisely this.

Unfortunately, the Risk Barometer also noted that 47 percent of the participating companies were less likely to execute the above activities implemented by the “very effective” companies. These companies have work to do.

Where does your company stand?

If you aren’t sure how your ERM capabilities stack up, you need to find out. Companies are advised to self-assess their ERM quality using S&P’s four components to ascertain whether any gaps exist. Gaps should warrant careful analysis to develop action plans that improve risk management capabilities. While analysts bring the bias of a creditor to the ratings process (and therefore place a stronger emphasis on protecting enterprise value), the capabilities needed to address their concerns are a step in the right direction and ultimately will benefit shareholders as well.

The self-assessment diagnostic should focus on whether the company has the following:

- An enterprisewide view of risks and a process for identifying the priority risks, with an organized catalog of risks, supported with definitions, readily available to provide a common risk language
- Policies and procedures in place for managing the priority risks within defined risk tolerances with clear ownership over, and accountability for, execution
- Ability to accurately track and manage the number and magnitude of loss events, including the ability to identify, measure and manage risk exposures and losses against established risk tolerances, track risk trends over time and, if possible, benchmark the company against industry data
- Demonstrated ability to avoid unexpected losses outside of established tolerance levels over time, with the objective of supporting a conclusion that the company is at least unlikely to experience such losses in the foreseeable future
- Clear evidence that risk and risk management capabilities are an integral part of strategy-setting and business planning, including the ability to relate key risk indicators (KRIs) to strategic objectives

A recurring theme throughout the S&P RFC is measurement. One indicator of robust ERM is having various measurement processes in place and functioning effectively. For example, in financial institutions the likely “currency” for ERM is economic capital, risk-adjusted return on capital, or something similar. In its RFC, S&P highlighted as a key differentiator in the aftermath of Katrina those firms that could quickly estimate losses with some measure of precision (within, say, 25 percent). Having information systems and processes in place to create relevant measures for managing risk exposures and losses within pre-determined risk tolerances will be vital for firms to progress to a rating of “excellent.”

A key objective for S&P appears to be reducing the *volatility* of losses. Accomplishing this objective may ultimately require sound modeling techniques and data-gathering and data-cleansing processes of both internal and external loss data. If companies are able to demonstrate excellent ERM quality, as defined by S&P, they likely will be seen as having less earnings and cash flow volatility and as optimizing the risk/return relationship. These companies are the ones most likely to be rewarded with a higher debt rating, which will drive reduced financing costs. For many nonfinancial companies, that impact would capture the attention of the C-Suite and the board.

Some best practices for working with the analyst

With respect to the ERM inquiry itself, we recommend the following practices:

- **Involve your CEO.** Your top executive’s point of view as to the importance of ERM in managing the business is vital to the analyst’s understanding of ERM quality. It is important that the CEO support the objective of transparency and open communications around risk and be committed to a risk-sensitive culture. It is a safe bet that the analyst will be looking for this.
- **Articulate your risk profile from a creditor’s point of view.** While *enhancing* enterprise value is important and the risk-taking associated with opportunity-seeking behavior is a relevant and important topic, the analyst’s primary emphasis is likely to be on *protecting* enterprise value and balancing opportunity-seeking behavior with risks undertaken. Therefore, describing the company’s risk profile with a creditor’s bias toward reducing the risk of unexpected losses will help place into context the conversation around the importance of ERM quality. For example, if the company enters into complex transactions with complicated risks and is highly leveraged, the analyst or an S&P ratings committee may place greater weight on the ERM score.
- **Describe your process clearly.** The analyst will want to understand the company’s process for identifying, measuring, managing and monitoring risk; review descriptions of risk-control programs for the priority risks; and note examples of their execution. Your description of the process should address how it is integrated with the company’s strategy-setting and business-planning processes and how it impacts corporate decision-making. Be sure to describe how your policies, infrastructure and methodologies support your risk management culture and related processes.
- **Focus on what makes sense to your business.** The analyst will not expect the company to do everything exactly in accordance with the S&P rating criteria. The ratings process is not a perfunctory “check-the-box” approach. The analyst will expect the company to vary its risk management capabilities according to its strategy, organizational structure, risk profile, risk tolerances and the complexity

of specific priority risks. So be prepared to state the company's point of view around the what, who, why and how of risk management.

- **Recognize the bar will continue to rise.** It is possible that there may not be a dramatic change in ratings in the first year of implementation. In the second year, however, there might be more variation among companies. Because we can expect the operating environment to continue to change, standing pat with respect to the company's risk management capabilities will not be a wise choice. Given the increasing complexity of both the business and risks over time, the analyst will undoubtedly want to see evidence of continuous improvement. As S&P benchmarks companies within a sector against one another, we can expect risk metrics, measurement tools and monitoring processes to emerge as key differentiators in company ERM quality ratings. Remember, the higher the

organization's risk appetite, and the more complex the risks taken by the organization, the more importance the analyst will assign to ERM quality. Ultimately, the analyst is evaluating his or her comfort level with how management looks at and evaluates risk, and determining whether anything is missing. So be prepared for the question: How do you know?

Summary

Nonfinancial companies can expect analysts to look for involvement of all levels of management in the ERM process. There has never been a better time or a better reason for most companies – financial and nonfinancial – to take a hard look at where their ERM practices stand. Given the potential positive or negative impact on financing costs, and the market perceptions, a proactive approach to evaluating and improving ERM quality is the most viable option.

Key Questions to Ask

Key questions for board members:

- Has management reported to the board on the status of the company's ERM process using the applicable rating service's PIM evaluation criteria? For example:
 - Do risk management policies cover such factors as risk tolerance, the company's internal and external reporting, and the processes for assessing financial and nonfinancial risk?
 - Does the risk management infrastructure address the processes, personnel, reporting and technology needed to manage critical risks and support risk communications at all levels?
 - Does the risk management methodology provide for appropriate metrics for assessing and quantifying risk and for incorporating risk into corporate decision-making?
 - Are you satisfied that the organization's risk management culture and governance are functioning effectively? Is there sufficient clarity around the roles, responsibilities and accountabilities of those responsible for risk management, and are they positioned appropriately within the organization to influence corporate decision-making?

Key questions for management:

- Have you self-assessed your company's ERM quality using the applicable rating service criteria (e.g., the four S&P components) to ascertain whether any gaps exist? If gaps do exist, have you developed an action plan to improve risk management capabilities on a timely basis?
- Do you know what your priority risks are? Have you compared your list of risks against the key risks S&P has identified for your industry? Have you considered emerging risks and your organization's ability to avoid losses in excess of established tolerances?
- Have you evaluated both the design and operating effectiveness of the policies, infrastructure and methodologies underlying your ERM process? If so, have you shared the results with the board?
- With respect to the priority risks, are they owned by someone or by some committee, function or unit empowered to act with clear accountability for results? Are these risks managed against established risk tolerances with the intent to reduce exposure to unexpected losses? Does the organization have effective risk measurement tools?

Need help preparing for the S&P credit ratings evaluation process? Whether you are identifying gaps, developing action plans to address known gaps or implementing remediation plans, Protiviti can help. We have worked with companies around the world to drive value from each step in this process. Call **1.888.556.7420** to speak with one of our Managing Directors regarding your ERM process and infrastructure or to learn more about the information covered in this issue of *The Bulletin* and what it means to your business.

Appendix C: ERM Panel Members

Susan Abeles* – Associate Vice Chancellor for Corporate Financial Services/Controller, UCLA
Joe Adams – EH&S Director, Risk Services, UCOP
Steven Beckwith – Vice President for Research & Graduate Studies, UCOP
Judy Boyette – Associate Vice President, HR & Benefits, UCOP
Anne Broome – Vice President, Finance, UCOP
Bob Charbonneau – Coordinator, Facilities Administration, UCOP
Paul Craig* – Chief Risk/Safety Officer, UCSDMC
Grace Crickette – Chief Risk Officer, Risk Services, UCOP
Al Diaz* – Vice Chancellor for Administration, UCR
Jon Good – Director, Systems Development, UCOP
Khira Griscavage* – Special Advisor to the Vice Chancellor for Administration, UCB
Kris Hafner – Associate Vice President, Information Resources & Communications, UCOP
Norman Hamill – University General Counsel, UCOP
Vicky Harrison – Chief of Police and Director of Public Safety, UCB
Don Larson – Assistant Vice Chancellor for Business & Financial Services/Controller, UCSD
Eugene Lau – Compliance Coordinator, Office of Research, UCSF
Jake McGuire – Controller, Agriculture and Natural Resources, UCOP
Mary Miller* – Vice Chancellor for Administration, UCM
Stan Nosek* – Vice Chancellor for Administration, UCD
Patrick Reed – University Auditor, UCOP
Dan Sampson – Director, Financial Controls and Accountability, UCOP
Patrick Schlesinger – Director, Research, UCOP
Sheryl Vacca – Senior Vice President & Chief Compliance and Audit Officer, UCOP

* Joined ERM Panel in May 2008.